*भारतीय मानक*
***Indian Standard***

**IS/ISO/TS 17574 : 2009**

# इलैक्ट्रॉनिक शुल्क एकत्रीकरण — सुरक्षा संरक्षण प्रोफाइल हेतु मार्ग-दर्शन

# Electronic Fee Collection — Guidelines for Security Protection Profiles

ICS 03.220.20; 35.240.60

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली–110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.org.in www.standardsbis.in

**September 2015** **Price Group 15**

Intelligent Transport Systems Sectional Committee, TED 28

## NATIONAL FOREWORD

This Indian Standard which is identical with ISO/TS 17574 : 2009 'Electronic fee collection — Guidelines for security protection profiles' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on the recommendation of the Intelligent Transport Systems Sectional Committee and approval of the Transport Engineering Division Council.

The text of ISO Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions and terminologies are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma ( , ) has been used as a decimal marker while in Indian Standards, the current practice is to use a point ( . ) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards, which are to be substituted in their places, are listed below along with their degree of equivalence for the editions indicated:

| *International Standard* | *Corresponding Indian Standard* | *Degree of Equivalence* |
|---|---|---|
| ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model | IS 14990 (Part 1) : 2012 Information technology — Security techniques — Evaluation criteria for IT security: Part 1 Introduction and general model (*second revision*) | Identical with ISO/IEC 15408-1 : 2009 |
| ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements | IS 14990 (Part 2) : 2006 Information technology — Security techniques — Evaluation criteria for IT security: Part 2 Security functional requirements (*first revision*) | Identical with ISO/IEC 15408-2 : 2005 |
| ISO/IEC 15408-3 : 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements | IS 14990 (Part 3) : 2006 Information technology — Security techniques — Evaluation criteria for IT security: Part 3 Security assurance requirements (*first revision*) | Identical with ISO/IEC 15408-3 : 2005 |

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 1960 'Rules for rounding off numerical values (*revised*)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

# *Indian Standard*
# 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.

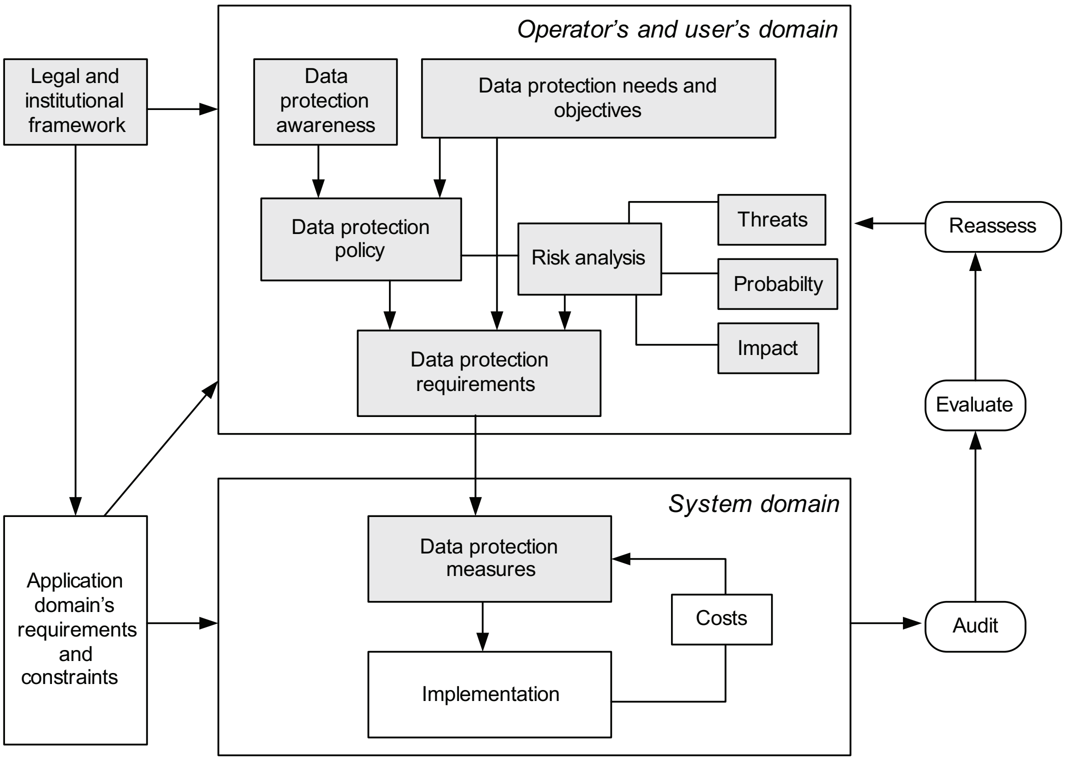
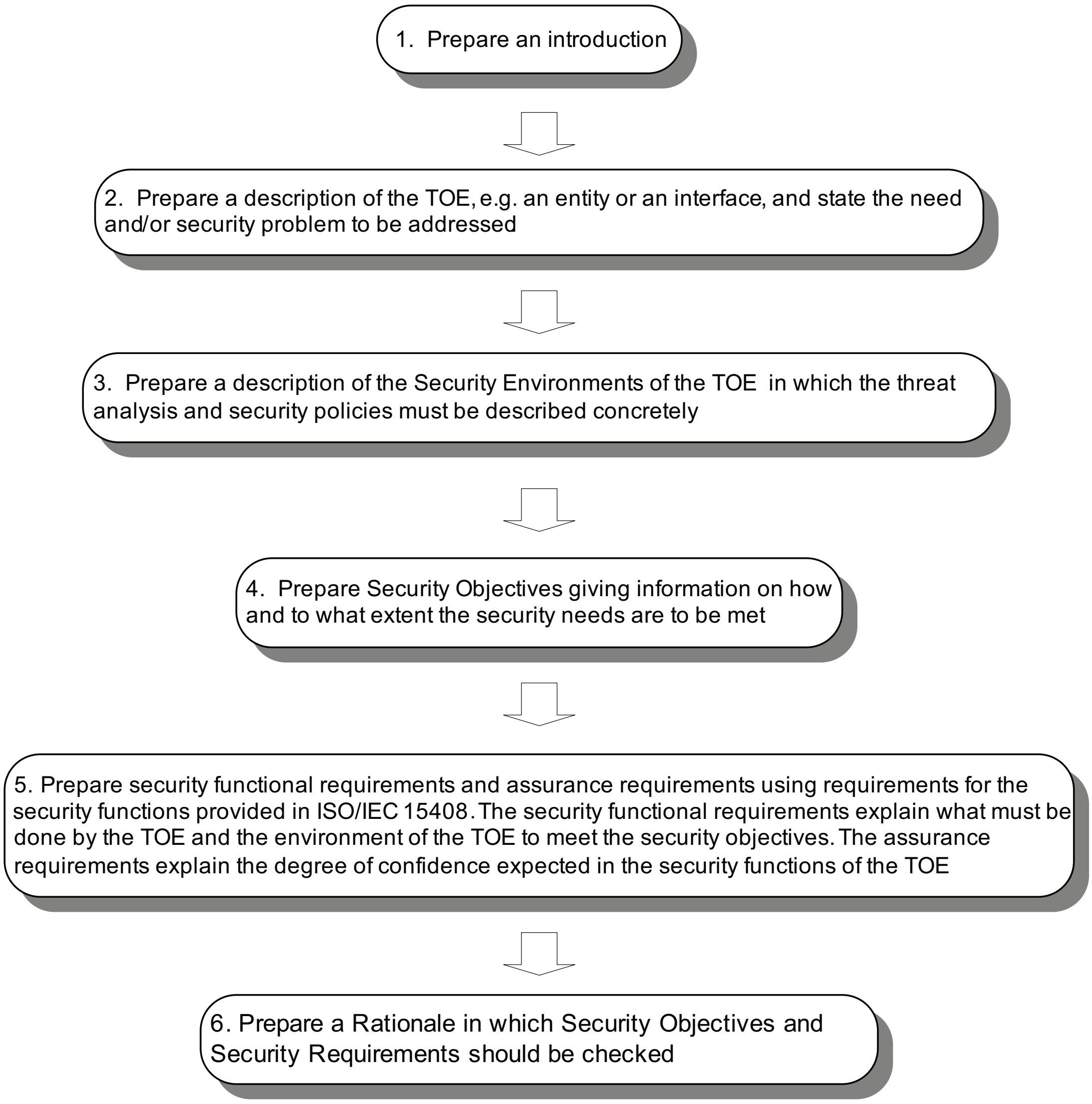

Operator's and user's domain
Legal and institutional framework
Data protection awareness
Data protection needs and objectives
Data protection policy
Risk analysis
Threats
Probabilty
Impact
Data protection requirements
Reassess
Evaluate
System domain
Data protection measures
Costs
Implementation
Application domain's requirements and constraints
Audit

**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).



1. Prepare an introduction

2. Prepare a description of the TOE, e.g. an entity or an interface, and state the need and/or security problem to be addressed

3. Prepare a description of the Security Environments of the TOE in which the threat analysis and security policies must be described concretely

4. Prepare Security Objectives giving information on how and to what extent the security needs are to be met

5. Prepare security functional requirements 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. Prepare a Rationale in which Security Objectives and Security Requirements should be checked

**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.

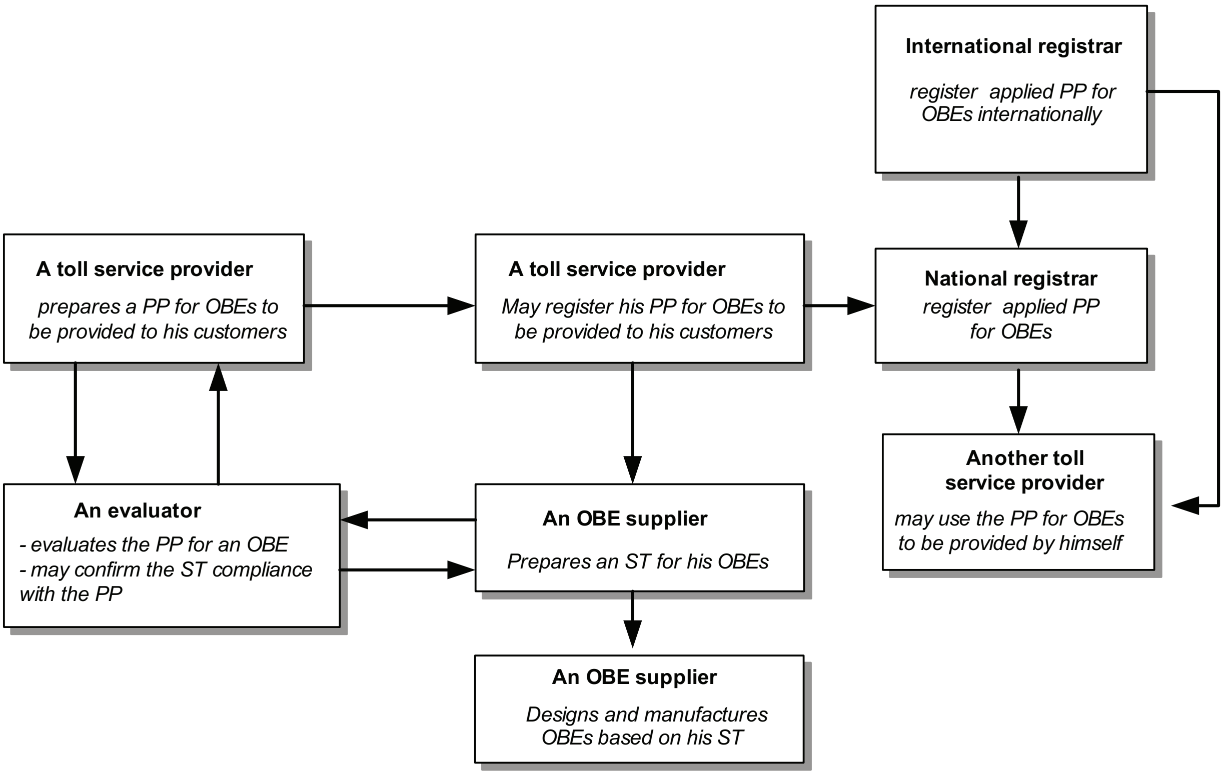

International registrar
register applied PP for OBEs internationally
A toll service provider
prepares a PP for OBEs to be provided to his customers
A toll service provider
May register his PP for OBEs to be provided to his customers
National registrar
register applied PP for OBEs
Another toll service provider
may use the PP for OBEs to be provided by himself
An evaluator
- evaluates the PP for an OBE
- may confirm the ST compliance with the PP
An OBE supplier
Prepares an ST for his OBEs
An OBE supplier
Designs and manufactures OBEs based on his ST

**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.

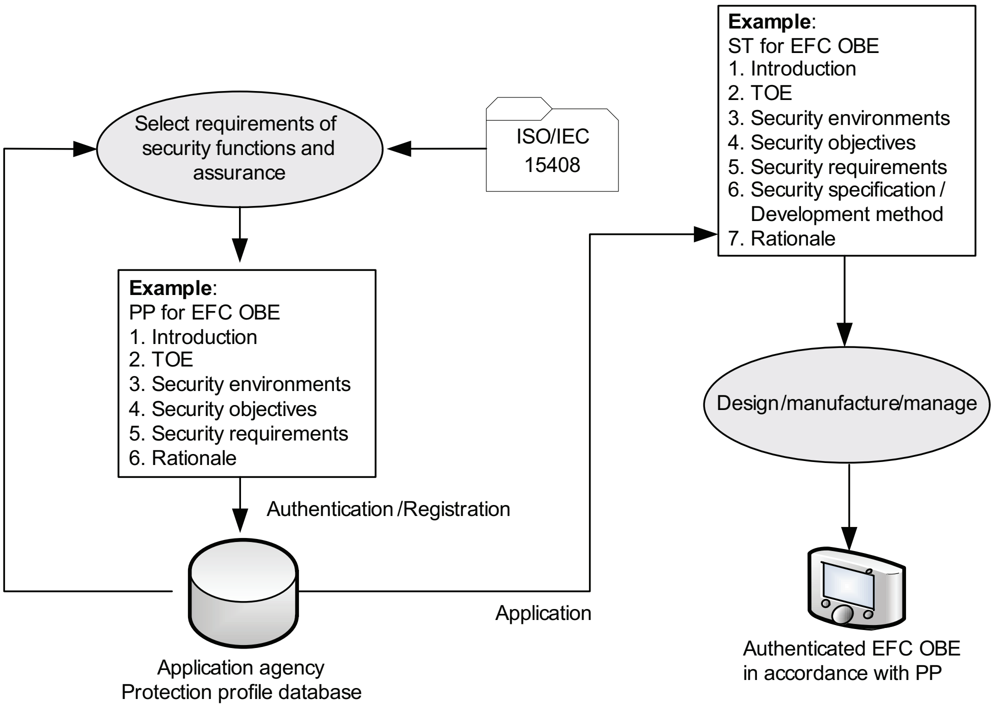


**Figure 4 — Example of design based on a PP**

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.

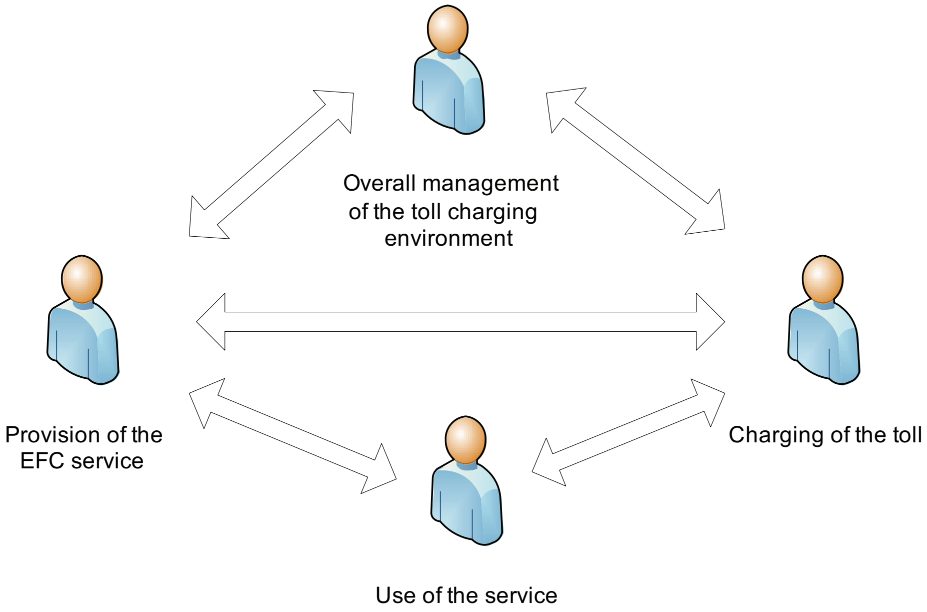

Overall management of the toll charging environment
Provision of the EFC service
Charging of the toll
Use of the service

**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.

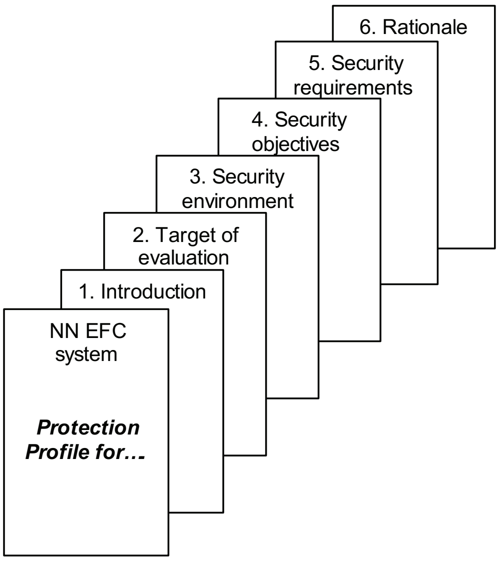


**Figure 6 — Content of a Protection Profile**

## 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.

Functional requirements are provided selecting necessary requirements from ISO/IEC 15408-2 and determining parameters.

Regarding assurance requirements, assurance requirements designated in ISO/IEC 15408-3 are adopted by determining evaluation levels for assurance requirements, which are provided in ISO/IEC 15408-2 and ISO/IEC 15408-3.

f) Rationale of justification/effectiveness (See Clause A.6).

The contents of PP are checked when necessary and cover security requirements for the TOE. The checked items are as follows:

1) all security environments needed are covered;

2) security objectives should completely meet the security environments;

3) security requirements should implement security objectives.

# Annex A
(informative)

# Procedures for preparing documents

## A.1 Introduction

### A.1.1 General

A general outline of the document for Protection Profile (PP) is described.

It should be noted that this clause is informative in nature. Most of the content is an example on how to prepare the security requirements for EFC equipment, in this case an OBE with a smart card (ICC) loaded with crucial data needed for the Electronic Fee Collection.

NOTE The examples are only that and nothing more.

### A.1.2 Identification information

Identification information for the document is as follows:

a) document title;

b) version/release number;

c) preparation date;

d) prepared by.

EXAMPLE Identification information:

1) document title: EFC On-Board Equipment Security Protection Profile;

2) reference/version number: 1.0;

3) preparation date: 2002-10-20;

4) prepared by: ABC Association.

### A.1.3 Target of evaluation (TOE) description

TOE is identified as follows:

a) product;

b) version/release number;

c) developer.

EXAMPLE TOE description:

1) product: EFC On-Board equipment;

2) version/release number: 1.0;

3) developer: ABC Co., Ltd.

### A.1.4 Accordance with the ISO/IEC 15408 series

The prepared “Protection Profile” in accordance with ISO/IEC 15408 is stated explicitly.

The version and preparation data of referenced ISO/IEC15408 documents are also stated.

EXAMPLE ISO/IEC 15408 conformance statement according to:

— ISO/IEC 15408-1 Second Edition 2005-09-22

— ISO/IEC 15408-2 Third Edition 2008-08-19

— ISO/IEC 15408-3 Third Edition 2008-08-19

### A.1.5 Outline of TOE

#### A.1.5.1 Classification of TOE

EXAMPLE

1.4.1 Classification of TOE

EFC On-Board Equipments

#### A.1.5.2 TOE functional outline

For users of security “Protection Profile”, the types of device described in “Protection Profile” are described explicitly to help them determine the application.

EXAMPLE

1.4.2 TOE functional outline (OBE for EFC system)

The functional outline is as follows.

a) EFC function:

   1) mutual authentication with IC card;

   2) transcription (caching) of IC card 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 IC card to OBE.

c) HMI function:

   1) report of EFC billing results to users;

   2) guidance of EFC lane.

#### A.1.5.3 Evaluation Assurance Level (EAL)

Evaluation Assurance Levels for objectives are selected. Each EAL defines a package consisting of assurance components and determines the degree of assurance requirements on security systems. The justification for the selected EAL is stated.

EXAMPLE

A.1.5.3 EFC OBE (EAL is 5)

OBE functions as equipment for e-Commerce in EFC transactions. The security systems of EFC OBE are vulnerable to attack under the control of individual users. Therefore, a high assurance level (EAL) will be required for EFC OBE.

## A.2 Target of Evaluation (TOE)

### A.2.1 TOE objectives and methodology

#### A.2.1.1 TOE use objectives

The following indicates objectives for TOE use and the type of environment in which it is used.

EXAMPLE EFC members (users) use the EFC system at tollgates by inserting the IC card with EFC member contract information for settlement. Vehicle information such as an automobile inspection certification is stored in OBE beforehand. For storing vehicle information, a personalization card for initialization is used. The OBE (TOE), which reads/writes data to IC cards for set-ups/settlements and transmits/receives data to roadside equipment for toll collection transactions, protects interface and internal data from external threats.

#### A.2.1.2 TOE use methodology

a) User preparations:

steps to be taken by users before use of TOE.

b) Operators preparation:

necessary hardware/software and control systems are described when operators operate TOE.

c) Operational procedures:

procedures for operation and maintenance are described.

d) Use procedures:

procedures for users are described.

e) Limitations of use:

limitations of use such as time zones and geographical zones are described.

EXAMPLE

a) User preparations:

Users request an operator to install an OBE and set-up vehicle information such as automobile inspection certification to OBE. In addition, users receive the ICC with EFC member contract information.

b) Operator preparations:

Operators issue set-up information in response to user’s requests.

c) Operation procedures:

When users are passing through tollgates, the tolls are billed to the IC cards for settlement with EFC member contract information, which is inserted in the installed On-Board Equipment with vehicle information. When a legitimate IC card for settlement is inserted in the OBE with correct vehicle information, the toll fee is calculated in the communication zone of RSE at tollgates.

For a change or update of EFC member contract information, such, as vehicle information, set-up cards and ICC are updated (reissued/reregistered).

d) Use procedures:

Users use the EFC system of inserting IC cards with EFC member contract information at tollgates according to the EFC member contract or OBE manuals.

e) Limitations of use:

In general, 24 h use is available, as long as EFC lanes are open at tollgates.

## A.2.2 TOE functions

### A.2.2.1 Functions provided by TOE

Functions, which are provided by the TOE, are described. All functions for data transactions, which must be protected, are listed.

EXAMPLE

a) EFC transactions

1) EFC communication control function;

2) non-secure data record function;

3) HMI input/output control function;

4) IC card insert status detect function;

5) On-Board Equipment self-check function.

b) Security module

1) data storage or protection function;

2) user access control function;

3) authentication function(DSRC, ICC);

4) encryption/decryption function;

5) ICC interface function;

6) EFC transaction interface function;

7) set-up card read function.

### A.2.2.2 Functions not provided by TOE

When the TOE function is a part of the functions of an entire system, the scope of the TOE in the whole system should be shown as in Figure A.1 which shows an example where the OBE is the scope of the TOE.

EXAMPLE

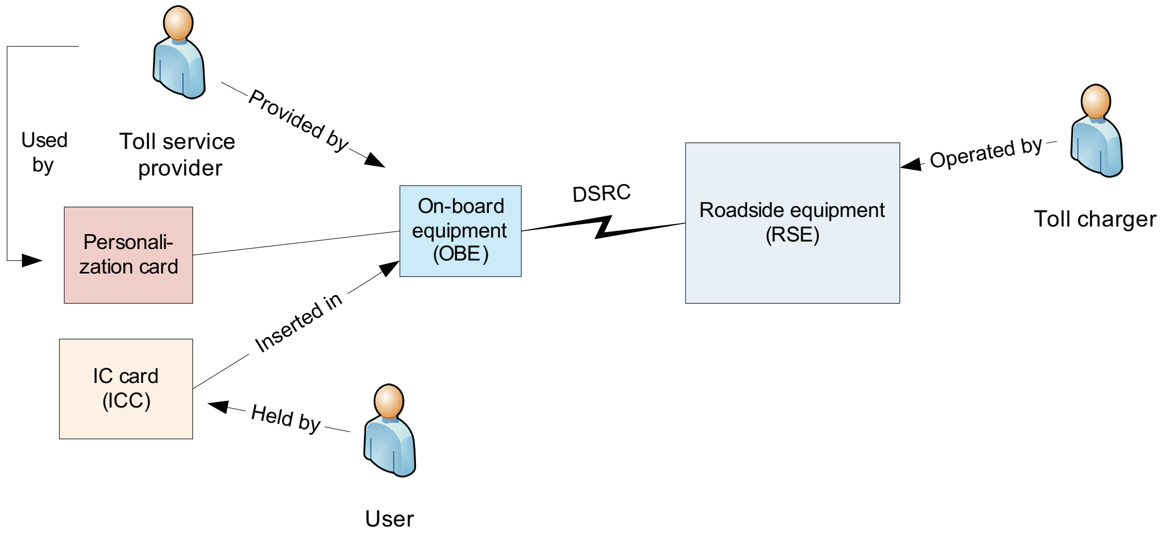


**Figure A.1 — An example where the TOE is shown in its context**

### A.2.2.3 Missing functions

When functions, which usually should be provided by the TOE in this section, are not included in the TOE, the function contents and reasoning for exclusion should be described.

## A.2.3 TOE structure

### A.2.3.1 Hardware structure

The structure with related hardware units on TOE operation is described. The scope of TOE in the structure should be shown as in Figure A.2.

EXAMPLE

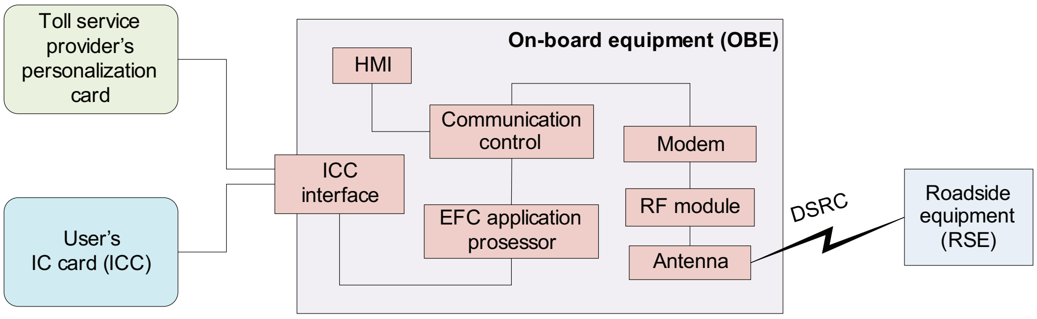


**Figure A.2 — An example of TOE hardware structure**

### A.2.3.2 Software structure

The structure with related software in the operation of the TOE is described. In the structure, the scope of the TOE in the structure should be stated. Especially, when the operation of the TOE depends on operating system (OS) and data control programs, the distribution of functions should be described.

#### A.2.3.3 Rationale

It should be verified that the described items are consistent.

a) Absence of inconsistent provision items.

b) Absence of undefined or unclear sections of provided contents in this clause.

## A.3 Security environment

### A.3.1 Operation/operational environment of TOE

#### A.3.1.1 General

Security requirements to determine security objectives for the TOE operation are provided.

#### A.3.1.2 Operational environments

The methodology of the use of the TOE such as the operational environment, operational time, operational site, use procedure and location of use is described. The described contents of A.2.1.2 are described in detail from the aspect of functionality.

a) Operational procedures

Regarding the operational procedures of the TOE, the operation of an integrated EFC system including the related vehicles and ICC for payment are described.

b) Operational time

The operational time zone of the TOE is described.

EXAMPLE The operational time is any time that EFC vehicles use on EFC toll roads

c) Operational sites

Operational sites of the TOE are described.

d) Use procedures

The procedures from the purchase (obtain) to the disposal of the TOE by users are described including installation of the TOE, set-up of the TOE and operation at toll roads.

EXAMPLE:

1) Users purchase EFC OBE at OBE dealers (car dealers, car shops). An OBE is installed in a vehicle. In addition, the On-Board information needed for the EFC operation such as vehicle information is stored as On-Board information.

2) After an EFC member contract is established, users get an ICC, which is issued by credit card companies.

3) Users will be able to use the EFC system by inserting an ICC in an OBE installed in a vehicle. The vehicles, which are capable of using EFC systems, are called EFC vehicles.

4) Users use toll roads with the ICC inserted in an OBE in an EFC vehicle and pass through the tollgates without stopping.

Users can voluntarily dispose of unnecessary OBE.

e) Use sites

Sites, where users are able to use TOE, are described.

EXAMPLE Toll roads, along which EFC RSE are installed.

f) Limits and requirements in use such as available numbers of TOE are described.

EXAMPLE

1) The number of OBE installed per vehicle is limited to one.

2) OBE are fixed (built-in) in a vehicle.

3) OBE can be used 24 h a day as long as EFC lanes are open for operation.

#### A.3.1.3 Physical control

Physical control related to the operation of the TOE is described.

a) Installation sites and control

Installation sites and physical control of the TOE are described.

EXAMPLE OBE is fixed (built-in) in a vehicle.

b) User unit

For use of the TOE, the physical control requirements of ICC for payments, which users possess, is described.

EXAMPLE Users are responsible for their ICC.

#### A.3.1.4 Personnel requirements

The personnel requirements for the responsibility and confidence of the TOE operations are described. In addition, the requirements for potential uses, motivations, methods and expertise of attacks are provided.

a) TOE related agents

The following items regarding the manufacturers, operators and users of TOE are stated.

1) Type

2) Role

3) Authorization

4) Reliance

5) Risk of illicit use

6) Expertise

7) Trail

EXAMPLE Personnel requirements:

Type: Manufacturer of On-Board Equipment.

Role: Manufacturing and shipping based on standard specification of EFC OBE.

Authorization: None.

Reliance: No responsibility for security control.

Risk of illicit use: There are risks of illicit use since the responsibility for security control is absent.

Expertise: No need of expertise for security.

Trail: Negative list check is implemented while EFC vehicles are passing through tollgates.

b) Attackers

The following items are described for illicit user requirements against which countermeasures are taken by the TOE

1) Type

2) Purpose of illicit use

3) Motivation

4) Means

5) Expertise

EXAMPLE Attackers:

i) Type: Illicit third party among EFC users.

ii) Purpose of illicit use: OBE data forgery, manipulation, obtaining of personal information. Forgery and illicit modification of OBE medium.

iii) Motivation: To reduce toll fees or avoid toll fee claims by illicit use of information. Sale of forged OBE.

iv) Means: Forgery of vehicle information on On-Board Equipments. Forgery of I/F data between OBE and ICC to counterfeit someone’s card. Forgery of EFC OBE by analysing OBE internally.

v) Expertise: Comprehend the internal transaction by analysing EFC On-Board Equipment internally.

### A.3.1.5 Connectivity/operational environments

The environment for TOE connectivity and operation is provided. Only the structure, which is provided in this subclause, shall be TOE.

a) Connectivity

Transactions for RSE at tollgates and ICC needed for the operation of the TOE are described.

EXAMPLE

— OBE exchange information via radio communication (5.8 GHZ) with RSE at tollgates.

— OBE-read IC card data (card number, ETC member contract information) before vehicles pass through tollgates. When vehicles pass through tollgates, OBE send applicable IC card internal data to RSE to transmit billing and transaction record data.

b) Operational requirements

Hardware/ software requirements needed for operation of the TOE are described.

(CPU implementation speed, required memory, input/output devices)

#### A.3.1.6 Rationale

It is verified that the described items are consistent.

a) Absence of inconsistent provision items.

b) Absence of undefined or unclear sections of provided contents in this subclause.

### A.3.2 Security threats

#### A.3.2.1 Determination of target resources for protection

a) Selection of target resources for protection

Target resources for protection, to be protected by the TOE, are determined. Resources, which negatively impact services of the TOE by falsification, alteration and loss, are targeted for protection. Regarding determined individual targeted resources for protection, the lifecycle such as generation, transaction, storage and disposal are clearly described. If there are indirect resources for a TOE transaction, the indirect resources are determined as well.

EXAMPLE

1) Target protection resources to be protected by the TOE:

- ETC member contract information: ICC internal data (i.e. IC card number);
- vehicle information: OBE internal data such as vehicle classification codes;
- tollgate information: exit/enter information, barrier information and transaction record information;
- information stated above, transmitted by radio communication through OBE between roadside units at tollgates and ICC;
- toll information: storage in ICC such as billing information.

2) Target resources for protection such as lifecycle:

- OBE installation in a vehicle;
- transcription of vehicle information into OBE;
- OBE operation at toll roads;
- OBE disposal.

b) Evaluation of target resources for protection

The values of determined target resources for protection are evaluated. The evaluation is divided into three levels as follows:

Level 1: security problems' impact on entire system for the TOE; e.g., the system might be malfunctioning or down.

Level 2: security problems drastically compromise the value of the system for the TOE; e.g., the social responsibility for the systems is impaired, however, restoration of systems is attainable.

Level 3: security problems hinder the operation of the TOE; e.g., operation of the system is temporarily interrupted resulting in serious impact on the users.

EXAMPLE

Evaluation of target resource for protection

Level 1: Non (no target resource for protection, which impacts systems such as destroying ETC systems);

Level 2: ETC member contract information;

Level 3: Vehicle information, tollgate information, toll information.

### A.3.2.2 Identification of security threats

Potential threats are identified by level of determined target resources for protection. Concrete analysis of target resource for protection is implemented in terms of who (what), where, when, how (counterfeiting, tapping, destruction), means (available resources, interface, expertise), threats (falsification, exposure, service interruption) and reasons.

a) Who (what):
who (what) generating threats is stated.

b) Target resource:
target resource for threats (billing data, personal information) is stated.

c) Contents of threats:
major threats are as follows.

1) Lack of confidentiality.

2) Lack of protection.

3) Lack of availability.

4) Lack of responsibility.

5) Lack of integrity.

6) Lack of reliability.

d) Means:
means generating attacks are stated.

e) Methodology:
methodology of attacks is stated.

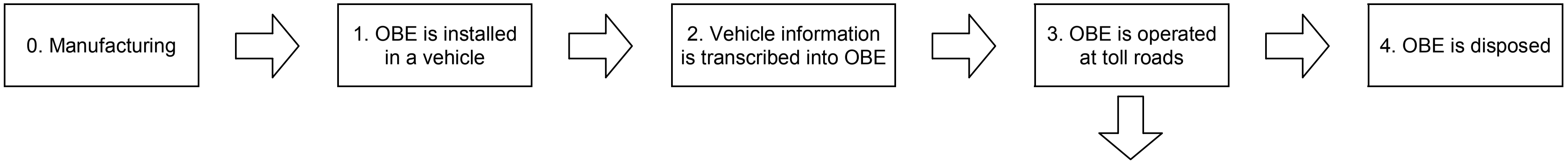
f) Motivation:
motivation of attacks is stated.

g) Opportunity:
opportunity of attacks is stated.

h) Weak points:
security weaknesses are stated.

Threat analysis for lifecycle of target data for protection is shown in Table A.1.

**Table A.1 — Threat analysis in lifecycle of ETC On-Board Equipment data for protection – An example**


0. Manufacturing
1. OBE is installed in a vehicle
2. Vehicle information is transcribed into OBE
3. OBE is operated at toll roads
4. OBE is disposed

Lifecycle: Threat analysis for “3. OBE operation at toll roads”

| Information for protection | Threat | | | | | |
|---|---|---|---|---|---|---|
| | Who | Where | When | Methodology, means | Threats | Why |
| ETC member contract information | Illicit third party | OBE | While inserting ICC | Forge ICC or I/F data to falsify someone’s card. | Forgery and altering of ICC internal data. | Avoid toll fee claim. |
| Vehicle information | | OBE | Anytime/while passing tollgates | Forgery of vehicle codes of OBE. | Forgery and manipulation of OBE internal data. | Reduce toll fee. |
| Tollgate information | | Tollgate lanes | Communication (billing) | Eavesdropping of radio communication.<br>Replay the eavesdropped data. | Tapping of radio communication data.<br>Communication data manipulation.<br>Replay attack. | Obtain personal information.<br>Reduce or avoid toll fee. |
| Toll fee information | | | | | | |

#### A.3.2.3 Rationale

It is verified that the described items are consistent.

a) Absence of inconsistent provision items.

b) Absence of undefined or unclear sections of provided contents in this subclause.

### A.3.3 Security policy of operational entity

#### A.3.3.1 General

Security items for operational entities for the TOE are provided in accordance with the rules and policies. The document names describing concrete rules are described.

#### A.3.3.2 Identification of security policies of operational entities

a) Use policy of target resource for protection

Use policy (to whom, what capability, when, where) for target resource of protections is provided.

b) Maintenance policy (update, disposal) of target resource for protection

c) Operational rules and applicable laws for security

i.e. Security policy based on “Law for prohibiting illicit access” is provided.

d) System and responsibility/duty for security policy

The security control/promotion system, responsibility and role are provided.

#### A.3.3.3 Rationale

Among security policy items of each operational entity, it is checked that there is no contradiction in the provision contents with the methodology and results being described.

a) Absence of inconsistent provision items.

b) Absence of undefined or unclear parts of provided contents in this subclause.

## A.4 Security objectives

### A.4.1 General

Regarding security threats listed in A.3.2, security objectives are determined from both aspects of technical objectives, which are provided by EFC systems or the operational environment of the EFC system, and operation control objectives.

### A.4.2 Technical security objectives

Technical security objectives provide security objectives, which are implemented by security functions such as encryption of data and control of access authentication.

a) For determination of security objectives, technical security objectives against threats are clearly described.

b) Security objectives are determined from the aspect of “control”, “prevention”, “detection” and “recovery”.

Control: the generation of security threats is controlled.

EXAMPLE Billing resource information such as EFC contract information is stored so securely in ICC and SAM installed in OBE for caching that it is protected from tampering.

Prevention: prevent security destruction when security threat is generated.

EXAMPLE Data is protected by encrypted data of radio communication information.

Detection: security threats are detected.

EXAMPLE Data falsification is detected by adding an authentication code to the message data.

Recovery: when security threats are detected, the original secure status will be restored.

EXAMPLE When a forgery of OBE or ICC is detected, negative information is recorded and the use is terminated. For legitimate users, a new OBE or ICC is reissued.

The following are some of the basic elements of security objectives.

1) Availability

   Information transaction resource is effectively used anytime anywhere, when needed. Major security objectives are as follows.

   i) Term of validity: setting the term of validity for IC cards, IC cards need to be changed periodically.

   ii) Damage control: equipment at tollgates controlling toll-billing information should have dual configuration to avoid being damaged.

   iii) Automation: personnel intervention for preparation of bills is eliminated.

2) Confidentiality

   Information is protected from illegal access.

   i) Access control:

      — operation capability of equipment is checked;

      — communication paths are checked.

   ii) Confidentiality of data: data of EFC member contract information/billing information is encrypted.

   iii) Encryption key management: generation of cryptographic key, distribution and storage are managed.

3) Protection

   Information is protected from illicit alteration or facilitation.

   i) Access control: usage capability of data and program library are checked.

   ii) Data flow control: logic space for data flow is provided; between internal networks and external networks, telecommunication data is filtered.

   iii) Data protection: data falsification and illegal addition of data/insertion of forwarding blocks are detected.

4) Legitimacy

Original information is verified. Communication document is verified to be the same original document. In addition, the records for resource use are verified.

i) Trace/audit: information for radio telecommunication is recorded as log data to be used to detect problems and for security objectives.

ii) Detection of security intervention: illicit interventions are detected in advance.

5) Traceability

Use status of target resource for protection is analysed and any unusual status is detected.

i) Identification/authentication: toll fees are charged to actual EFC users through identification/authentication.

ii) Session control: radio communication paths are protected from illicit intervention.

iii) Privacy: EFC contract information and use information are protected from exposure.

iv) Security entity protection: security entities are checked for bypass or interference.

6) Common requirements

Common requirements for security objectives are as follows.

i) Digital signature: E-signature is required for verification for EFC contract information.

ii) Time stamps: transaction date of billing information is recorded.

iii) Transmission denial prevention: sent or received transactions are recorded as verification.

### A.4.3 Security objectives by TOE

a) Identification of security objectives

Contents of security objectives are described in detail. Requirements in A.3 to be implemented are described with rationale. In addition, the expected degree to which the security objectives meet the security environments is also described with rationale.

b) Rationale

Checking that no contradiction exists between security objectives, which were identified in a) and the rationale contents and results are described.

1) Absence of inconsistent provision items.

2) Absence of undefined or unclear parts of provided contents in this subclause.

### A.4.4 Security objectives by operation environment of TOE

a) Identification of security objectives

Contents of security objectives are described in detail. The requirements in A.3 to be implemented are described with rationale. In addition, the expected degree of security objectives to meet the security environments is described with rationale as well.

b) Rationale

Checking for the absence of contradiction among security objectives, which were identified in a) and the rationale contents and results are described.

1) Absence of inconsistent provision items.

2) Absence of undefined or unclear sections of provided contents in this subclause.

### A.4.5 Rationale

Checking that no contradiction exists among security objectives, which were identified in A.4.1 and the rationale contents and results are described.

1) Absence of inconsistent provision items.

2) Absence of undefined or unclear sections of provided contents in this subclause.

**Table A.2 — TOE Security Objectives —– An example**

| No. | Threats | Security objectives | | | |
|---|---|---|---|---|---|
| | | Control | Prevention | Detection | Recovery |
| 1 | Forgery and altering of OBE (media)<br>(Analysing the OBE, forgery of the OBE media and implementation of illicit communications transactions with RSE) | Information unit control (anti-tampering) | Identification/authentication<br>Access control | Data protection (message authentication) | User control (negative list record) |
| 2 | Forgery and falsification of OBE data<br>(Forgery vehicle information in OBE to reduce communication fees) | Operational control (Check vehicle information at EFC member contract and the data is also checked by roadside units) | Data confidentiality (encryption function)<br>Control of term of validity (check validated term of data) | Data protection (message authentication) | User control (negative list record) |
| 3 | Forgery and altering of prepaid ICC<br>(Analysing prepaid ICC, alteration of the prepaid ICC, which is not withdrawn) | Information unit control (anti-tampering) | Identification/authentication<br>Access control (limitation) | Trail audit (telecommunication log audit) | User control (negative list record) |
| 4 | Forgery and altering of ICC data<br>[Forging ICC data or I/F data, counterfeiting a legitimate user's card (postpaid) or increase the usage value (prepaid)] | Information unit control (anti-tampering) | Data confidentiality (encryption function)<br>Access control | Trail audit (telecommunication log audit) | User control (negative list record) |
| 5 | Forgery and altering of RSE<br>(Forging RSE, theft of personal data from ICC) | Operational control<br>(Personal information on radio communication between RSE and OBE is not to be recorded) | Data confidentiality (encryption function)<br>Privacy<br>(Protection of EFC member contract information/usage information)<br>Access control | Detection of security intervention (illicit intervention detection)<br>Data protection (message authentication) | Encryption key control (update of key information) |

**Table A.2** *(continued)*

| No. | Threats | Security objectives | | | |
|---|---|---|---|---|---|
| | | Control | Prevention | Detection | Recovery |
| 6 | Tapping of radio communication contents<br>(Tapping radio telecommunication waves between OBE and RSE, obtaining personal information) | Session control (illicit intervention countermeasures) | Data confidentiality (encryption function)<br>Privacy<br>(Protection of EFC member contract information/usage information) | Physical control of tollgate facilities (periodic patrols) | Encryption key control (update of key information) |
| 7 | Forgery and falsification of telecommunication data<br>(Falsifying telecommunication data contents, transmission of the falsified data at tollgates to reduce the toll fees) | Session control (illicit intervention countermeasures) | Data confidentiality (encryption function) | Data protection (message authentication)<br>Trail audit (communication log audit) | Encryption key control (update of key information) |
| 8 | Multiple usage of OBE<br>[With installation of several OBEs in one vehicle, repeating communication transactions and obtaining several transaction data for one use (defrauding toll fees)] | OBE usage control (ban on installation of several OBEs for one vehicle by usage provision of contract) | Data flow control<br>(checking the number of vehicles and OBEs)<br>Validated term control (checking validated term)<br>Time stamp | Trail audit (communication log audit) | Time stamp (control of outdated information) |
| 9 | Poor connection or intentional outset of ICC<br>(Physical or digital interruption of telecommunication between OBE and ICC; personnel action for drawing out ICC, accidental poor connection) | Usage control of OBE (ban and penalty rules for drawing out ICC by provision of the contract) | Access control<br>(OBE/ICC software locking) | Trail audit<br>(ICC transaction verification) | Reissuing of ICC |
| 10 | Malicious usage of repeating radio telecommunication waves eavesdropped at tollgates (avoiding toll fees by repeating communication transactions eavesdropped at tollgates) | Session control (illicit intervention countermeasure) | Timestamp<br>Data flow control | Data protection (communication control) | Time stamp (control of outdated information) |
| 11 | OBE theft/loss (illicit use of stolen or lost OBE) | Physical control (strengthening of OBE installation methodology) | Access control (negative information control for theft report) | Trail/audit (communication log audit) | User control (negative information record, reissuing) |
| 12 | ICC theft/loss (avoiding toll fees charged by loss of ICC) | ICC usage control (state ICC control responsibility by usage provision of contract) | Access control (negative information control for theft report)<br>Identification/authentication (authentication by owner) | Trail/audit (communication log audit) | User control (negative information record, re-application) |

**Table A.2** *(continued)*

| No. | Threats | Security objectives | | | |
|---|---|---|---|---|---|
| | | Control | Prevention | Detection | Recovery |
| 13 | Theft or duplication of usage application<br>(illicit use of personal information through theft or duplication of usage application) | Information usage control<br>Physical control of application | Authentication/Identification (authentication by owner) | Physical control (storage control of application) | |
| 14 | Jamming<br>(jamming near tollgates to interrupt the operation) | Policy for jamming | Operation control (access control, supervision and patrol of tollgates) | Operation control (i.e. patrol) | |
| NOTE Security objectives for from 1 to 10 of threats are performed by technical measures. Those for from 11 to 14 are performed by operational control. | | | | | |

## A.5 Security requirements

### A.5.1 Overview of ISO/IEC 15408

Part 1 defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives and for selecting and defining IT security requirements.

Security requirements are defined in Parts 2 and 3 of ISO/IEC 15408; Part 2 for functional requirements and Part 3 for assurance requirements. Both requirements are described in the same structure in that they are defined hierarchically by the units labelled Class, Family and Component. The relationship between those units is shown in Figure A.3.

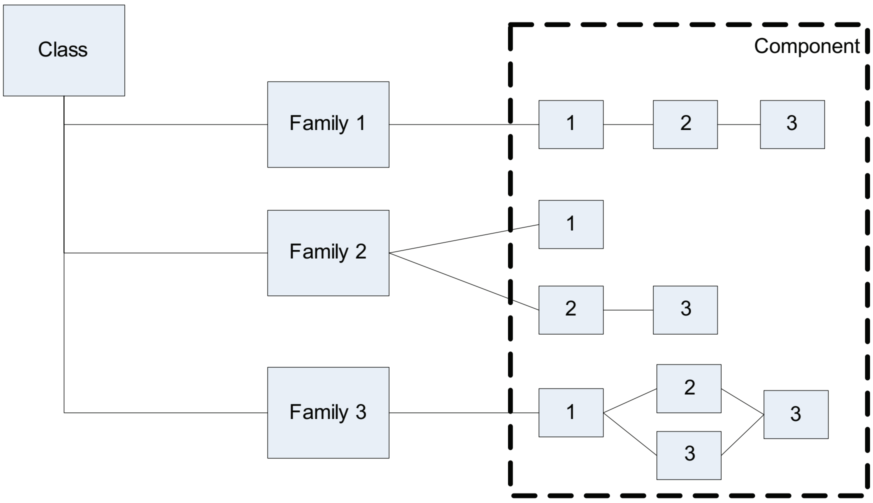


**Figure A.3 — Relationship between units that define requirements**

Class is the most general unit that defines security requirements. Families in a class share common security objectives.

Family is a set of security requirement units that share common security objectives. Each component in a family has possible differences in its emphasis and exactness.

Component is a set of specific security requirements which also shows the minimum set of requirements. It could be sub-divided into elements, each of which could constitute one component. It can be either hierarchical or non-hierarchical as shown in Figure A.3.

Security requirements can be defined by using ISO/IEC 15408, based on selection of class, family and component.

Security functional requirements are shown in Table A.3, while whole classes and families of security assurance evaluation are in Table A.4.

As indicated in Tables A.3 and A.4, three letters represent class and family individually.

**Table A.3 — Security functional requirements — From ISO/IEC 15408-2**

| Function class | Function contents | Function family | |
|---|---|---|---|
| FAU<br>Security audit | Security requirements for audit log control | ARP | Security audit automatic response |
| | | GEN | Security audit data generation |
| | | SAA | Security audit analysis |
| | | SAR | Security audit review |
| | | SEL | Security audit event selection |
| | | STG | Security audit event storage |
| FCO<br>Communication | Assurance requirements for transaction record of communication and legitimate communication data contents | NRO | Non-repudiation of origin |
| | | NRR | Non-repudiation of receipt |
| FCS<br>Cryptographic support | Requirements for cryptographic key management (except cryptographic algorithm) | CKM | Cryptographic key management |
| | | COP | Cryptographic operation |
| FDP<br>User data protection | Requirements to protect user data | ACC | Access control policy |
| | | ACF | Access control functions |
| | | DAU | Data authentication |
| | | EFC | Export to outside TSF control |
| | | IFC | Information flow control policy |
| | | IFF | Information flow control functions |
| | | ITC | Import from outside TFS control |
| | | ITT | Internal TOE transfer |
| | | RIP | Residual information protection |
| | | ROL | Rollback |
| | | SDI | Stored data integrity |
| | | UCT | Inter-TSF user data confidentiality transfer protection |
| | | UIT | Inter-TSF user data integrity transfer protection |
| FIA<br>Identification/ authentication | Requirements to identify users and verify the legitimate user | AFL | Authentication failures |
| | | ATD | User attribute definition |
| | | SOS | Specification of secrets |
| | | UAU | User authentication |
| | | UID | User identification |
| | | USB | User-subject binding |

**Table A.3** *(continued)*

| Function class | Function contents | Function family | |
|---|---|---|---|
| FMT<br>Security management | Requirements for security functional management | MOF | Management of functions in TSF |
| | | MSA | Management of security attributes |
| | | MTD | Management of TSF data |
| | | REV | Revocation |
| | | SAE | Security attribute expiration |
| | | SMR | Security management roles |
| FPR<br>Privacy | Requirements for privacy | ANO | Anonymity |
| | | PSE | Pseudonymity |
| | | UNL | Unlinkability |
| | | UNO | Unobservability |
| FPT<br>Protection of TOE security functions | Requirements to protect security system from illicit interference | AMT | Underlying abstract machine test |
| | | FLS | Fail secure |
| | | ITA | Availability of exported TSF data |
| | | ITC | Confidentiality of exported TSF data |
| | | ITI | Integrity of exported TSF data |
| | | ITT | Internal TOE TSF data transfer |
| | | PHP | TSF physical protection |
| | | RCV | Trusted recovery |
| | | RPL | Replay detection |
| | | RVM | Reference mediation |
| | | SEP | Domain separation |
| | | SSP | State synchrony protocol |
| | | STM | Time stamps |
| | | TDC | Inter-TSF TSF data consistency |
| | | TRC | Internal TOE TSF data replication consistency |
| | | TST | TSF self test |
| FRU<br>Resource utilization | Assurance requirements for stable provision of resource services | FLT | Fault tolerance |
| | | PRS | Priority of service |
| | | RSA | Resource allocation |
| FTA<br>TOE access | Requirements to prevent illicit use of information transaction products and systems | LSA | Limitation on scope of selectable attributes |
| | | MCS | Limitation of multiple concurrent sessions |
| | | SSL | Session locking |
| | | TAB | TOE access banners |
| | | TAH | TOE access history |
| | | TSE | TOE session establishment |
| FTP<br>Trusted path/channels | Requirements to secure communication paths between security systems and users | ITC | Inter-TSF trusted channel |
| | | TRP | Trusted path |

**Table A.4 — Security assurance evaluation — From ISO/IEC 15408**

| Assurance class | Assurance family | | Necessary assurance components | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 |
| APE<br>PP evaluation | DES | TOE description | (Independent on EAL) | | | | | | |
| | ENV | Security environment | | | | | | | |
| | INT | PP introduction | | | | | | | |
| | OBJ | Security objectives | | | | | | | |
| | REQ | Security requirements | | | | | | | |
| | SRE | Explicitly security requirements | | | | | | | |
| ASE<br>ST evaluation | DES | TOE description | (Independent on EAL) | | | | | | |
| | ENV | Security environment | | | | | | | |
| | INT | ST introduction | | | | | | | |
| | OBJ | Security objectives | | | | | | | |
| | PPC | PP claims | | | | | | | |
| | REQ | Security requirements | | | | | | | |
| | SRE | Explicitly security requirements | | | | | | | |
| | TSS | TOE summary specification | | | | | | | |
| ACM<br>Configuration management | AUT | CM automation | | | | 1 | 1 | 2 | 2 |
| | CAP | CM capabilities | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | SCP | Tracking of updated information | | | 1 | 2 | 3 | 3 | 3 |
| ADO<br>Delivery/operation | DEL | Delivery | | 1 | 1 | 2 | 2 | 2 | 3 |
| | IGS | Installation, generation and set-up | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ADV<br>Development | FSP | Functional specification | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | HLD | High-level design | | 1 | 2 | 2 | 3 | 4 | 5 |
| | IMP | Implementation representation | | | | 1 | 2 | 3 | 3 |
| | INT | Source/object cord | | | | | 1 | 2 | 3 |
| | LLD | Module structure | | | | 1 | 1 | 2 | 2 |
| | RCR | Representation correspondence | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | SPM | Security policy modelling | | | | 1 | 3 | 3 | 3 |
| AGD<br>Guidance | ADM | Administrator guidance | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | USR | User guidance | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ALC<br>Life cycle | DVS | Development security | | | 1 | 1 | 1 | 2 | 2 |
| | FLR | Flaw redemption | | | | | | | |
| | LCD | Security for development/protection | | | | 1 | 2 | 2 | 3 |
| | TAT | Development, operational tools | | | | 1 | 2 | 3 | 3 |
| ATE<br>Tests | COV | Coverage | | 1 | 2 | 2 | 2 | 3 | 3 |
| | DPT | Depth | | | 1 | 1 | 2 | 2 | 3 |
| | FUN | Functional tests | | 1 | 1 | 1 | 1 | 2 | 2 |
| | IND | 3rd party testing | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| AVA<br>Vulnerability assessment | CCA | Cover channel analysis | | | | | 1 | 2 | 2 |
| | MSU | Misuse | | | 1 | 2 | 2 | 3 | 3 |
| | SOF | Strength of security function | | 1 | 1 | 1 | 1 | 1 | 1 |
| | VLA | Vulnerability analysis | | 1 | 1 | 2 | 3 | 4 | 4 |
| AMA<br>Maintenance of assurance | AMP | Assurance maintenance plan | (Independent on EAL) | | | | | | |
| | CAT | TOE component categorization report | | | | | | | |
| | EVD | Evidence of assurance maintenance | | | | | | | |
| | SIA | Security impact analysis | | | | | | | |

By referring to Tables A.3 and A.4, an example of component selection regarding functional requirements and assurance evaluations is described as follows.

- Security functional requirement

Component selection is implemented according to Table A.3. In the case of "generation of cryptographic key" as an example of security objective, FCS (cryptographic support) is selected among function classes. CKM (cryptographic key management) is selected among function families. Then FCS_CKM.1 (generation of cryptographic key) is selected as component.

- Security assurance evaluation

The necessary components for security assurance evaluation are automatically determined in ISO/IEC 15408-3, once Evaluation Assurance Level (EAL) is selected.

Here component is selected with reference to Table 5 of ISO/IEC 15408-3:2008.

Suppose EAL is 4 as assurance class, ACM (configuration management) is selected. Then assurance family consists of AUT (configuration management automation), CAP (configuration management capabilities), and SCP (tracking of updated information). Necessary assurance components are indicated in each EAL in Table 5 of ISO/IEC 15408-3:2008.

Components of "configuration management" (EAL4) are:

- ACM.AUT.1
- ACM.CAP.4
- ACM.SCP.2

## A.5.2 TOE functional requirements

### A.5.2.1 Relevant functional requirements and parameter determinations

Relevant functional requirements are selected from ISO/IEC 15408-2 to embody TOE technical security objectives. Selection is implemented at component levels.

The structure of ISO/IEC 15408-2 is as follows (parts provided in ISO/IEC 15408-2 are shown in italics):

- FDP User data protection

  This is a provided unit labelled **"Class".**

- Information flow control functions (FDP_IFF)

  This is a provided unit labelled **"Family"**.

With this unit, the following requirements for management and audit are provided.

*Management: FDP_IFF.1, FDP_IFF.2.*

*The following actions could be considered for the management functions in FMT management:*

The listed components (in this case: FDP_IFF.1, FDP_IFF.2) must meet the requirements for management provided above.

Audit: FDP_IFF.1, FDP_IFF.2, FDP_IFF.5.

*The following events should be auditable if FAU_GEN Security audit data generation is included in a PP/ST.*

a) *Minimal:* *Decisions to permit requested information flows*

b) *Basic:* *All decisions on requests for information flows*

c) *Detailed:* *The specific security attributes used in making an information flow enforcement decision.*

The listed components (in this case, FDP_IFF.1, FDP_IFF.2, FDP_IFF.5) must meet the requirements for audits provided above.

Target events for audit are selected from a), b) and c). The events of the contents, which are provided at each level, should be collected as an audit log.

*FDP_IFF.2 Hierarchical security attributes*

This is a **component.**

Hierarchical to: FDP_IFF.1

This demonstrates hierarchy of components. In the case selection of this component (FDP_IFF.2), the following components, which are shown in this clause, should not be selected (in this case, FDP_IFF.1). All the following component requirements are included in this component.

*FDP_IFF.2.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment : the minimum number and type of security attributes].*

*FDP_IFF.2.2 The TSF shall permit an information flow.*

*FDP_IFF.2.7 The TSF shall enforce the following relationships.*

This is an element group. Elements for each element are provided in detail. Parameters (assignment) are designated. For instance, in *FDP_IFF.2.1* above, *information flow control SFP* is designated in detail. In addition, the frequency and type for *the minimum number and type of security attributes* are designated in detail.

Dependencies: FDP_IFC Subset information flow control

*FMT_MSA.3 Static attribute initialization*

Components related to this clause are shown.

Basic procedures for selecting functional requirements are described as follows:

a) Selecting functional requirements directly needed for implementing security objectives

For instance, Family "FIA_UAU: User authentication" in Class "FIA: Identification/Authentication" of ISO/IEC 15408-2 is selected for the security objective "User Authentication". Then the component "FIA_UAU.3: Unforgettable authentication" is selected.

Two elements for this component are provided as follows:

— FIA_UAU3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.

— FIA_UAU3.2 The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.

The appropriate event for parameter “selection”, which is included in this requirement, is designated. For other parameters such as “assignment”, an event is provided in detail.

Thus, the functional requirements needed for all the security objectives are selected. The general content of functional requirements provided in ISO/IEC 15408-2 are shown in Table A.3.

b) Selecting functional requirements interdependent with selected functional requirements

Although “FIA_UAU.3: unforgettable authentication” stated above, list “no dependencies”, each functional component provides a complete list of dependencies on other functional and assurance components. For instance, in the case when “FDP_IFF.2”, “FDP_IFC.1 Subset information flow control” and “FMT_MSA.3 Static attribute initialization” are designated. These requirements are also selected. When the requirements depended upon in turn have dependencies on other requirements, all the requirements depended upon are selected.

c) Selecting necessary functional requirements for selected functional requirements for regular function

There are four functions to assure normal operation as follows:

- blocking bypasses of functions;
- rejecting interference of functions;
- assuring operations;
- detecting improper operations.

Blocking bypasses of functions: this function prevents security threats by bypassing the transaction of relevant functional requirements. In general, FPT_RVM.1 (Non-bypassability of the TSP) is selected. In addition, regarding bypassing of “user authentication”, the illicit use (bypassing) will be rejected by verifying user authentication through “access control”.

Rejecting interference of functions: this function stops interference in functional transactions by destroying or falsifying security attribute/data regarding relevant functional requirements. In general, FMT_MTD.1 (management of TSF data), FMT_MSA.1(management of security attributes), FPT_PHP (physical protection) FPT_SEP(domain separation) and FTP_TRP (trusted path) are selected.

Assuring operations: this function assures operation of relevant functional requirements. In general, FMT_MOF.1 (management of security functions) is selected.

Detecting improper operations: this function detects the operation of relevant functional requirements in an incorrect configuration or connection status. In general, audit function is selected.

d) Audit and management requirements are provided for each functional requirement

Corresponding to functional requirements, the type of audit log data to be collected is provided in ISO/IEC 15408-2. In the case of selecting the audit log data collection (e.g. FAU_GEN.1), provided requirements for collection are also selected. For instance, in the case of “FIA_UAU.3” stated above, audit is selected in the family, which includes the component for “FIA_UAU.3”. Therefore, the component is targeted and the collection levels of log data are selected from “Minimal” and “Basic”.

Minimal: detection of fraudulent authentication data.

Basic: all immediate measures taken and results of checks on fraudulent data.

e) Requirements for “Law for ban on illicit access” are provided

Functional requirements (FTA_TAB.1) for sending warning message to bar illicit access. In general, “Identification of security policy of operational entity” is selected in accordance with the law stated above.

#### A.5.2.2 Selection of strength of function (SOF)

When AVA_SOF is selected as the assurance requirement (when EAL2 is selected, this requirement is included), the SOF level is selected for functions which are provided by TOE. Target functions are functions to introduce technical security methodology such as combination of information and arrangement, or probability theory methodology. Requirements for cryptography are non-target for this level of strength of function.

Evaluation of attack potential

First of all, attack potential is evaluated. Attack potential is classified as follows:

- **SOF-basic:** attacks within an adequate period using interfaces which are open to the public.
- **SOF-medium:** attacks by attackers who are especially knowledgeable, within an adequate period using interfaces which are not open to the public.
- **SOF-high:** attacks within an attenuate period using special resources.

SOF levels

ISO/IEC 15408 provides three SOF levels to minimize attack potential as follows:

**Basic level:** this can protect secret information against attacks within an adequate period using interfaces which are open to the public.

EXAMPLE The following represents basic levels of strength of functions regarding passwords:

- more than six letters, combinations of numbers, letters and notations;
- in the case of more than three input password mistakes the transaction is cancelled.

Generation and input of false passwords are possible using an interface, which is open to the public. When the countermeasures stated above are implemented, attacks that have been executed for a couple of days can be defended against.

**Middle level:** this can protect secret information from attacks within an adequate period with expertise of security functions.

EXAMPLE The following represents middle level of strength of function regarding passwords:

- passwords are stored within IC cards with ten decimals, which are selected at random from different kinds of multiple letters;
- IC cards are under the control of each user.

Passwords are basically to be memorized by users. The basic level of strength of function is not capable of halting attacks by attackers who are especially knowledgeable of analogy. However, generating passwords at random can defend against this type of attack.

**High level:** this can protect secret information from attacks using special resources and oppose high level attacks.

“High level” of strength of function cannot be made available for passwords.

Without using the definition of ISO/IEC 15408, new evaluation methods can be defined.

Selection of SOF levels

Strength of function is selected for functional requirements. Strength levels are determined depending on sophistication of attackers in terms of expertise, available resources and motivations of attacks.

Minimum SOF level and validity:

this strength of function selects the minimum level of functional requirements of TOE. The justification of selected appropriateness of the SOF level should be addressed by the aspect of expertise, available resources and motivations of attacks.

SOF level by individual functional requirement and validity:

SOF level can be selected for individual functional requirements. Higher level is selected if an individual functional requirement is more eminent than the TOE in all. The justification of the selected appropriateness of the SOF level should be addressed by the aspect of expertise, available resources and motivations of attacks.

#### A.5.2.3 Rationale

a) Integrity: it is verified that all the parameters for functional requirements are selected. However, in order to give flexibility for preparation of “Security Target”, parameters can be kept intact.

b) Accuracy: it is verified that functional requirements accurately describe ISO/IEC 15408. It is also verified that selected parameters are not originally changed.

c) Validity: validity that determination contexts of parameters is appropriate, is explained.

d) Dependency: it is verified that dependency between functional requirements is satisfied. When dependency is not satisfied, the reason the security issue will not occur is explained.

e) Complement: it is verified that each function should not be interfered with illicitly, bypassed or interrupted. It is also checked that functions, which enable comprehension of the operational status, are determined. In general, for interference prevention, FPT_SEP (domain separation) is selected. For bypass prevention, FPT_RVM (reference mediation) is selected.

f) Correspondence: it is verified that at least one security functional requirement corresponds to each objective described in “Technical Security Objectives”. In addition, it is verified that there is no functional requirement, which doesn’t correspond to any of those objectives.

g) Opposition: it is verified that corresponding security objectives can be implemented using security functional requirements, which are provided in this subclause.

h) Consistency: it is verified that there is no contradictory determination between functional requirements and the rationale contexts and results described.

i) Availability: it is verified that each functional requirement can be implemented under “TOE operational requirements”

### A.5.3 TOE assurance evaluation

#### A.5.3.1 Assurance level

Functional requirements are individually selected at the component level as security requirements to enforce security objectives. However, in the case of assurance requirements, as a principle, only the assurance requirements that the TOE must satisfy, are selected. Regarding the selection, appropriate assurance levels are selected considering the operational environment, value of target resource for protection, technical realization, cost/period for development/evaluation and market demand.

Regarding assurance requirements, usually, only assurance levels (EAL) are determined. Necessary assurance requirement components are provided corresponding to each EAL in advance in ISO/IEC 15408-3.

Fundamental means of selection are as follows:

- protection of information transaction system from attacks for general commerce using interface, which is open to the public (EAL4);
- highly reliable protection of the information transaction system such as the user authentication service (EAL5);
- protection of commercial information transaction, in which the use environment is not open to the public, such as an in-company information transaction system (EAL3).

Corresponding components to selected assurance levels are determined in ISO/IEC 15408-3. Assurance requirements, which are provided in ISO/IEC 15408-3, and assurance components needed for each EAL are shown in Table A.4.

#### A.5.3.2 Added assurance components

Without determining the assurance level, components can be selected individually. In addition, components, which are not included in selected EAL levels, can be added as the need arises.

#### A.5.3.3 Rationale

It is verified that selected assurance levels are appropriate, neither too high nor too low, from the aspects of security environments or security objectives. For instance, suppose that measures of protection from threat agents with expertise in TOE transaction contents are security objectives. In this case, AVA_VLA.1, which doesn't require an analysis of clear vulnerability, is not an appropriate assurance requirement. AVA_VLA.2, requires the rationale of full protection from illicit use.

In addition, it is verified that selected assurance levels can be implemented by technical and financial aspects.

#### A.5.3.4 Selection example of OBE security functional requirements

A part of security functional requirements, which was prepared based on provision of OBE security objectives in A.4, is described in Table A.6. Here the selection procedure of security functional requirements is explained according to Table A.6. As security objectives, “information unit control (anti-tampering)” and “identification/authentication” are singled out.

Security functional requirements are selected among the following, defined in ISO/IEC 15408-2.

- Information unit control (anti-tampering)

  For this security objective, OBE is physically protected by exclusive LSI, which is tamper-proof in order to protect security.

  Here FPT (protection of TOE security functions) is selected as Function Class. PHP (TSF physical protection) is selected as Function Family. FPT_PHP.1 (passive detection of physical attack) is selected among FPT_PHP.1, FPT_PHP.2, and FPT_PHP.3 as Component of FPT_PHP. There is no management requirement defined for the component. Only one audit requirement is defined. “a) Minimal: if detected by IT means detection of intrusion” is thus selected as audit requirement.

- Identification/authentication

  For this security objective, OBE is authenticated in order to prevent usage of forged OBE.

Here FIA (identification/authentication) is selected as function class. UAU (user authentication) is selected as function family. Among seven components of FIA_UAU, FIA_UAU.3 (unforgettable authentication) is selected. There is no management requirement defined for the component. “a) Minimal: Detection of fraudulent authentication data” is selected as audit requirement. Selection of components of FTP_ITC.1 is omitted.

As indicated in the two examples above, security function requirements, compared to security objectives, are defined by selection of the following, described in ISO/IEC 15408-2:

- function class;
- function family;
- component (or element, if necessary);
- management requirement;
- audit requirement.

## A.6 Rationale of justification/effectiveness

### A.6.1 General

In this clause, the contents of “Protection profile” are checked to determine the necessity and the satisfaction of security requirements for the TOE. The items checked are shown as follows:

- all security environments needed are covered;
- security objectives should meet security requirements completely;
- security requirements should implement security objectives.

In this section, the rationale of the items, which are considered in A.1 to A.5, is identified.

### A.6.2 Rationale of security objectives

#### A.6.2.1 General

Regarding A.4, needs and sufficiency are verified.

#### A.6.2.2 Needs

It is verified:

- that there is more than one security objective for each item in the security requirements, which are provided in the identified TOE operational requirements, security threats and organizational security policy in Clause 5; this guarantees that all security objectives needed to realize security requirements are covered;
- that each security objective corresponds to more than one security requirement item;
- that unnecessary security objectives, which correspond to security requirements, are not included; redundant security objectives may generate security destruction risks.

NOTE It is easier to verify security objectives with a matrix describing the relationship between security requirements and security objectives. An example of such a matrix is given in Table A.5. Operational requirements and organizational security objectives are verified in the same way.

**Table A.5 — Threats and security objectives — An example**

| Security objectives | Threats | |
|---|---|---|
| | Forgery or altering of OBE media | Forgery or falsification of OBE inter-data |
| Information unit control (anti-tampering) | O | — |
| Operational control (check at vehicle information set-up) | — | O |
| Identification/authentication | O | — |
| Access control | O | — |
| Data confidentiality (encryption key control) | — | — |
| Expiration control (checking validity of data) | — | O |
| Data protection (message authentication) | — | O |
| User control (negative list record ) | O | O |
| O = applicable;<br>– = not applicable. | | |

### A.6.2.3 Sufficiency

It is verified:

- that security objectives are effective for individual threats; e.g., justifications are needed for “detecting threats and the capacity for the ability to recover” or “the ability to prevent or reduce the impact of threats at a permissible level”;
- that security objectives enable satisfaction of connective/operational requirements and organizational policies. It is also verified that security objectives of relevant operational environments are provided compatibly.

EXAMPLE Rationale of security objectives (sufficiency)

- Threat: by analysing ETC On-Board Equipments, forging OBE and executing illicit communication transactions with RSE.

  In order to prevent the above threat, the forged OBE, either through communication transaction or communication data, needs to be detected as well as protected from the altering of OBE. Security objectives such as “information unit control (anti-tampering)”, “identification/authentication”, “access control” or “user control (negative list record)” should be sufficient to prevent this threat.

- Threat: forging vehicle information in an OBE to reduce toll fees.

  In order for protection against threats, falsification of transmitted communication transaction data and communication data needs to be prevented or detected. The prevention from falsification of storage data in OBE also needs to be secured. Security objectives such as “operational control (checking of vehicle information)”, “confidentiality of data”, “checking validity period (expiration of valid data)”, “data protection (message authentication)” and “user control (negative list record)” are sufficient to prevent threats.

## A.6.3 Rationale of security functional requirements

### A.6.3.1 General

Security functional requirements are verified for the following aspects.

#### A.6.3.2 Needs

It is verified:

- that there is more than one security functional requirement to satisfy technical security objectives;
- that each functional requirement corresponds to more than one security objective.

NOTE It is easier to verify security functional requirements with a matrix describing the relationship between technical security objectives and security functional requirements. An example of such a matrix is give in Table A.6.

**Table A.6 — Rationale of security functional requirements (needs)**

| Functional requirements | Security objectives | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Information unit control (anti-tampering) | Identification/ authentication | Access control | Data confidentiality | Expiration control | Data protection | User control (negative list record) | Remarks |
| FIA_UAU.3<br>(User authentication) | — | ○ | — | — | — | — | — | – |
| FTP_ITC.1<br>(Inter-TSF trusted channels) | — | ○ | — | ○ | — | ○ | — | – |
| FDP_ACC.1<br>(access control policy) | — | — | ○ | — | — | — | — | – |
| FDP_ACF.1<br>(access control functions) | — | — | ○ | — | — | — | — | – |
| FDP_UCT.1<br>(Inter-TSF user data confidentiality transfer protection) | — | — | — | ○ | — | — | — | – |
| FPT_ITC.1<br>(Confidentiality of TSF data) | — | — | — | ○<br>(security data) | — | — | — | – |
| FDP_UIT.1<br>(Inter-TSF user data integrity transfer protection) | — | — | — | — | — | ○ | — | – |
| FPT_ITI.1<br>(Integrity of TSF data) | — | — | — | — | — | ○ | — | – |
| FPT_PHP.1<br>(TSF physical protection) | ○ | — | — | — | — | ○<br>(security data) | — | – |
| FMT_SAE.1<br>(Security attribute expiration) | — | — | — | — | ○ | — | — | – |
| FTA_TSE.1<br>(TOE session establishment) | — | — | ○ | — | ○ | — | ○ | – |
| (FTA_NLC.1) New requirement | — | — | — | — | — | — | (○) | – |
| (FTA_VTC.1) New requirement | — | — | — | — | (○) | — | — | – |
| FDP_DAU.1<br>(Data authentication) | — | — | — | — | — | ○ | — | – |
| ○ = applicable; (○) = potentially applicable; – = not applicable. | | | | | | | | |

### A.6.3.3 Sufficiency

The rationale for each security objective to be sufficiently prescribed by the provided functional requirements is explained. In particular, an explanation is given as to how functional requirements are operated for security objectives or how dependency between relevant functional requirements fits in with security objectives.

EXAMPLE Security functional requirements (sufficiency)

Security objectives: sufficiency of selected functional requirements for authentication.

Sufficiency:

- rationale of authentication is executed by checking exchanged data;
- rationale of authentication is prescribed by FIA_UAU.3 (functional requirements).

Data are certified using authenticators, which are generated from cryptographic keys and algorithms shared in the OBE and the RSE.

### A.6.3.4 Complement

It is verified that security functional requirements complement each other and that no contradiction is generated due to the complement:

- there are functional requirements to bypass for the operation of relevant functional requirements by other functional requirements;
- there are functional requirements to control the interference of relevant functional requirements by other functional requirements;
- there are functional requirements to control the illicit operation of relevant functional requirements by other functional requirements;
- there are functional requirements to verify that relevant functional requirements are not operated in the wrong status by other functional requirements.

**Table A.7 — Example of A.2 — Rationale of security functional requirements (complement)**

| **Functional requirements** | **Requirements to provide security defense** | | |
|---|---|---|---|
| | Blocking of bypasses | Non-interference | Non-operation controls |
| FIA_UAU.3 | FDP_ACF.1 | FPT_PHP.1 | N/A |

Security functional requirements (complement)

Complement

Blocking of bypasses: FDP_ACF.1

Security requirements to protect data using access control functions. Bypasses are blocked by installing access control functions in the module that is tamper-proof.

Non-interference: FPT_PHP.1

Security requirements to protect data from illicit interference using physical security functions. Illicit interference is prevented by installing security functions in the module that is tamper-proof.

Non-operation controls: N/A = Not applicable.

#### A.6.3.5 Availability

It is verified that each security functional requirement is realized under the TOE operational requirements. Availability is verified from the aspect of use, management and operation.

EXAMPLE Security functional requirements (availability):

Possibility of realization

Functional requirements: FIA_UAU.3

OBE data are enciphered by a third party and stored in the module that is tamper-proof. In the case of ETC use, data authentication between ICC and RSE with cryptographic keys provided by the same third party is implemented. Use of the ETC system is rejected when the authentication between the ICC and the RSE is not valid.

#### A.6.3.6 Mutual consistency of security functional requirements

It is verified that security functional requirements are consistent with each other. The relationship between functional requirements is dependence, refinement or augmentation, which indicates the absence of contradiction with the provided contents.

#### A.6.3.7 Dependency of security functional requirements

When there is dependency at the component level, it is verified that all the related components are selected.

### A.6.4 Rationale of strength of functions

In the case of requiring security functional strength (including AVA_SOF.1), the validity is explained from the aspect of motivation of threats, resources and countermeasure techniques.

### A.6.5 Rationale for security assurance requirements

- Validity of assurance levels

  It is verified that target assurance levels are not too low for identified threats.

  Concrete evaluation for the validity of target assurance levels is conducted based on: 1) level of attack potentials on the TOE; 2) assurance degree for the TOE operation/operational environment; 3) TOE users (specified or unspecified); 4) impact degree on peripheral environment when TOE security has been destroyed; 5) impact on development cost; 6) competition with other companies.

- Realization of assurance levels

  It is verified that target assurance levels can be realized from technical and financial aspects.

### A.6.6 Rationale of control/operational requirements

The validity for control/operational requirements is explained.

### A.6.7 Rationale of assurance methodology

Assurance requirements corresponding to each assurance methodology are clearly shown. It is explained that assurance means meeting assurance requirements. In addition, it is explained that the content is appropriate for the operation.

It is verified that sentences that are required by each assurance requirement exist and the contents of them are sufficient.

# Annex B
(informative)

# Example of threat analysis evaluation method

## B.1 Identification of threats

### B.1.1 General

Threats can be divided into the following three general categories:

a) intentional threats (attacks);

b) administrative threats;

c) accidental threats.

### B.1.2 Intentional threats (attacks)

Intentional threats are those that are made by malicious intruders (third parties). They can be classified into the following three categories:

a) fraudulent use of equipment;

b) alteration of accumulated data;

c) interception and abuse of personal data.

### B.1.3 Administrative threats

Administrative threats are those that are caused by a lack of security in administration and management, the abuse of privileges and EFC. These threats can be classified into the following three categories:

a) intrusion into the subscriber/user database;

b) tapping of personal data in the network;

c) fraudulent access into system databases or network control functions.

### B.1.4 Accidental threats

Accidental threats are those that are caused by operational errors by the user and communication transmission errors.

## B.2 Estimation of risks

a) Likelihood of occurrence

| | |
|---|---|
| — those individuals lacking expertise | 5 |
| — those individuals with expertise | 4 |

| | |
|---|---|
| — those groups possessing expertise | 3 |
| — those groups possessing expertise with sizable investment | 2 |
| — those company level parties with expertise | 1 |

1. Impact value

| | |
|---|---|
| — immense damage via system destruction (unrestorable) | 5 |
| — immense damage via limited system destruction (restorable) | 4 |
| — specified/unspecified users economically afflicted as a result of double or triple charging (loss of credit) | 3 |
| — leakage of charging data with continuation and expansion (involved parties are afflicted) | 2 |
| — leakage of charging data without continuation (involved parties are afflicted) | 1 |

2. Exposure factor

The exposure factor is calculated by multiplying a) by b).

## B.3 Evaluation and determination of countermeasures

### B.3.1 Evaluation method

The threats are evaluated by the above threat classification (A > B > C) and risk value.

**Table B.1 — Evaluation method**

| Classification | Likelihood of occurrence | Impact value | Exposure factor |
|---|---|---|---|
| A | 3 | 3 | 9 |
| B | 4 | 2 | 8 |

### B.3.2 Determination of security countermeasures

A threshold value is established for each threat identification in order to determine whether or not to carry out any security countermeasures. If the risk value equals or exceeds the threshold value, then security countermeasures should be carried out. Examples of the values are given as follows.

EXAMPLE

- threshold value A $\geqslant$ 5;
- threshold value B $\geqslant$ 10;
- threshold value C $\geqslant$ 15.

## Table B.2 — Threat analysis result for users (OBE and ICC interfaces) — an example

| | Objects of attacks | Outlines | Who | When | Where | What | Why | How | Functions for security improvement | Victims | Classification | Likelihood of occurrence | Impact value | Exposure factor |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | OBE | Forgery and falsification of OBE modules | Dishonest 3rd party | Anytime | | OBE | Reducing tolls,<br>sale of forged OBE | Analysing legitimate OBE and forging the modules, implementing false communication transaction with RSE | Authentication, anti-tampering, access restriction | Toll road operators<br>OBE manufacturers | A | 2 | 2 | 4 |
| 2 | OBE | Forgery and falsification of OBE internal data | Dishonest 3rd party | Anytime, while passing EFC lanes | | OBE | Reducing tolls | Forging vehicle model data in OBE to reduce tolls | Encryption function, message authentication, road side judgement check, check expiration date of data | Toll road operators | A | 4 | 2 | 8 |
| 3 | OBE | Theft and loss of OBE | Dishonest 3rd party | Anytime | Where OBE is installed and kept | OBE | Self-use,<br>sale to 3rd party | Theft | Enhancement of fixed method for vehicles, management using theft reports | OBE manufacturers<br>Users | A/C | 5 | 1 | 5 |
| 4 | ICC | Forgery and falsification of ICC modules | Dishonest 3rd party | Anytime | | ICC | Making unlimited use of prepaid cards for self use or sale to 3rd party | Analysing microchips inside legitimate prepaid cards to forge them for unlimited use | Authentication, tampering, access restriction | Toll road manufacturers<br>Card issuers | A | 2 | 4 | 8 |
| 5 | ICC, OBE/ICC interface | Forgery and falsification of OBE internal data | Dishonest 3rd party | Anytime, while inserting ICC | | ICC | Toll charges avoided (billing system) and unlimited use (prepaid system) | Forging the microchip of ICC and the data on interface as well as masquerading as another user (billing system) or increasing the usage value (prepaid system) | Authentication, encryption function, road judgement check, access restriction | Toll road operators<br>Card issuers | A | 4 | 2 | 8 |
| 6 | ICC | Theft and loss of ICC | Dishonest user<br>Honest user | Anytime | Where ICC is distributed and stored | ICC | Toll charges avoided | Theft | Management using theft reports, individual vigilance | Users<br>Toll road operators (no debts)<br>Card issuers | A | 5 | 3 | 15 |
| 7 | OBE and ICC | Acquisition of personal data | Dishonest 3rd party | Anytime | Where OBE and ICC are installed, distributed and stored | OBE, ICC | Illicit use of personal data | Forging RSE and reading the data from OBE and ICC at will | Authentication, encryption function, access restriction | Users | A | 2 | 3 | 6 |
| 8 | OBE/ICC Interface | ICC Transaction interference | Dishonest users<br>Honest users | While passing tollgates, while accessing ICC | Lanes at toll gates (in-vehicle) | OBE-ICC interfa ce | Abusing data without updating the ICC, interfering with system to allow unlimited card usage (intentional), and careless errors (unintentional) | Physically and electrically interfering with OBE-ICC communication on interface (running through ICC, intentional faulty contact) or accidental faulty contact | ICC transaction verification, OBE and ICC software lock | Toll road operators | A | 5 | 2 | 10 |

# Annex C
(informative)

# Abstract from *Definition of threats and security controls for the Charging Interface in Electronic Fee Collection*

NOTE The terminology used in this Annex may differ from the terminology used in the main body of the document as well as Annex A and B. As Annex C is an abstract of CEN/TC278 N780 *Definition of threats and security controls for the Charging Interface in Electronic Fee Collection*, it has been decided that the same terminology should be used in the abstract as in the original document.

## C.1 Introduction

### C.1.1 General

In Electronic Fee Collection (EFC) systems large amounts of data are handled, such as payment related data, enforcement related data, contract related data, EFC. Large parts of these data demand severe measures to protect them against fraud and privacy violation. If different operators want to share information or to enable each other's customers to use the system of the other, interoperability issues should be solved first. One of the aspects in this is data protection/security. If both operators have implemented different data protection/security schemes this might cause severe problems or even make interoperability impossible. An operator is willing to serve users having contracts with other operators by making his systems open to accept them as long as this does not imply weakening the strength of the data protection/security of his system.

If data protection/security in a system is based on the fact that all measures taken in the system to establish this are not public, but only known on a need-to-know basis, the strength of the data protection/security will become weaker by definition if information of the data protection/security measures is shared by more people (operators). Hence data protection/security in interoperable systems should be based on the strength of data protection/security schemes and not on the limited insight on its technicalities. Widespread knowledge of the data protection/security schemes should not weaken specific implementations. This can be reached by using modern data protection techniques, such as cryptographic algorithms and sophisticated key-management schemes.

To enable interoperability of systems, all data protection/security schemes implemented should fit into the same framework. This framework should describe the threats that are considered, define the set of security services that protect against these threats, and the ways these services are implemented via proper security mechanisms.

More details on such a data protection/security framework are given below.

### C.1.2 Security framework

#### C.1.2.1 Security requirements

The first step in establishing a security framework is to identify the different security requirements of the different EFC applications. Different applications, such as, for example, open and closed toll collection, may have a lot of identical requirements, but also some that are specific to the particular application. Generally, requirements will state that sufficient protection against a specific threat to the system should be provided. Some will call this security principles or the security profile.

#### C.1.2.2 Security services

The next step is to define the security services that may fulfil the required security profile, or, in other words, provide measures to protect against threats. Security services that are envisaged are, for example:

- access control service, providing protection against unauthorized operations on information or processes in the system;
- authentication services:
  - peer entity authentication, providing corroboration that the identity of a peer entity in an association is as claimed; e.g. IC card to road side equipment authentication, user to card authentication, EFC (also called segment authentication);
  - data origin authentication, providing corroboration that the identity of a source of data received is as claimed; e.g. the IC card provides proof that it is the origin of the data send (also called message authentication);
- confidentiality service, providing protection against unauthorized disclosure of information; applicable for data in transfer (e.g. data sent to and from the IC card or road side system), and for stored data (e.g. data stored on the IC card);
- integrity service, providing protection against unauthorized modification or deletion of information; also applicable both for data in transfer and stored data.

Other services could be defined, but in most cases they can be considered as specific limitations to a certain type of data of the generic security services defined above.

#### C.1.2.3 Security mechanisms

The third step is to describe the security mechanisms or security functions that can be used to implement the security services. This is a difficult step as there are many mechanisms that can be used to offer a particular service, each with its own strengths, weaknesses and limitations. It is also possible to offer more than one security service with a particular mechanism. A security framework should specify the mechanisms, point to existing standards of how to implement these mechanisms for EFC applications and how to synchronize in a conversation such that communication between two entities (e.g. a smart card and a road side system) with common security mechanisms becomes possible.

The available mechanisms should be incorporated in a security framework. Using this framework an operator could uniquely specify to a possible user which security measures are allowed and can be handled by his specific application. Furthermore, operators can make agreements under which security conditions one is going to accept claims from the other because the other has serviced a user from the former.

The number of security mechanisms should be as small as possible to ease interoperability, but on the other hand should be large enough to satisfy anyone's needs in a cost-effective way. Furthermore possibilities should be kept open to add new security mechanisms later on and to implement mechanisms not within the standard if one wishes.

## C.2 Scope

CEN/TC 278/WG 1 as an application oriented working group and deals with threats to the applications they define and the required countermeasures to protect against these threats. Hence, CEN/TC 278/WG 1 will specify the security services needed and, if the corresponding security mechanisms are already defined by other standards, how they should be used. Because threats to EFC systems depend on the actual size, geographical location and possible gain, no single set of security services can be defined. Instead, a framework of security profiles and services/mechanisms should be composed from which EFC systems can choose. The number of security profiles should on the one hand be as small as possible to ease interoperability, but on the other hand should be large enough to satisfy anyone's needs in a cost-effective way.

This Technical Specification defines the relevant EFC entity model. From a security point of view it will restrict itself to the charging interface between service provider and user using the DSRC link as communication medium. This, from an interoperability point of view, has the highest priority. For at least this interface, standards have to be available to enable interoperability, also from a security point of view.

The above mentioned restriction to the charging interface does not mean that the other interfaces are without serious fraud threats. Further work has to be done to consider the security of the entire system.

## C.3 EFC model

To start a threat analysis and definition of security services needed a model is required. To the five entity model in CEN/TC 278/WG 1/N 110 two extra entities are added. These are the exception handling operator and a so-called trusted third party. The exception handling operator is an abstract entity that is supposed to get involved by any other abstract entity in the model if an exception occurs. The trusted third party is an abstract entity that is introduced to assist in a number of security services that might be implemented. One could think of distribution and management of cryptographic keys, authorization and audit. The seven entity model with the relevant interfaces is shown in Figure C.1.

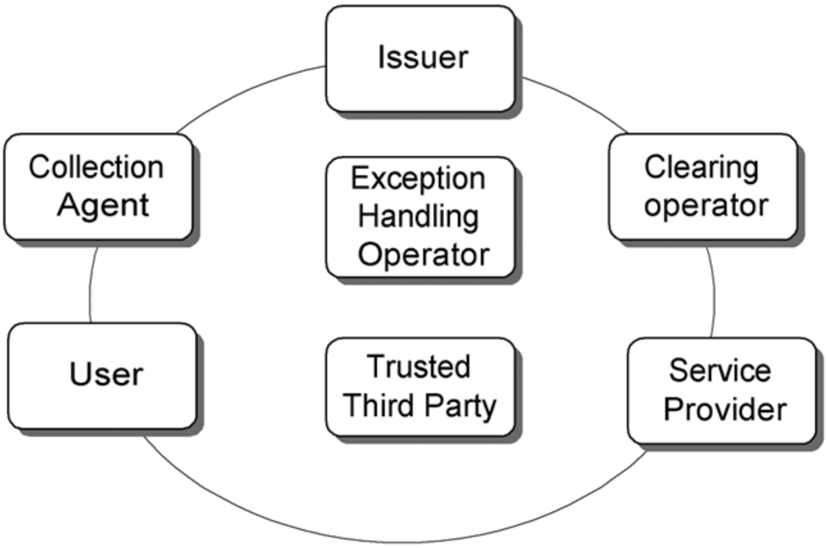


**Figure C.1 — Seven entity abstract model for EFC**

## C.4 Security and privacy requirements/targets

A complete list of generic security and privacy requirements in Electronic Fee Collection (EFC) systems should be determined such that individual security and privacy profiles can be composed by taking a subset of those requirements and by making them more specific for the particular EFC system to be built. This then defines a particular security policy.

The main requirements that the security architecture of an EFC system has to uphold are:

- it shall not be possible to debit or credit purses/accounts in a way not intended by the issuer;
- it shall not be possible to exchange value without agreement between the participants involved (e.g. the user and the service provider, or the user and the collection agent);
- it shall not be possible for participants to defraud others without detection;
- the balanced exchange of value shall be possible;

- recovery procedures in the event of error shall be available;
- adequate data to resolve conflicts shall be provided;
- the privacy of users involved in transactions shall be assured according to the data protection policy and the contracts.

A number of threats is associated with these requirements. They are discussed in the next clause.

## C.5 Threat analysis

### C.5.1 General

For the EFC system, a threat analysis should be performed. The frequency of the occurrence of threats and the expected damage a threat can cause determine the risk associated with that threat. The larger the risk the higher the level of (security) protection should be. Hence in a particular EFC system to each threat a risk can be associated. Consequently one can specify a requirement that a protection measure against the threat should be implemented in the form of a certain security service of a particular strength.

In this clause we will focus on the threats on the charging interface. The reason for this choice is the fact that it is the interface that will be more subject to threats than the other interfaces due to its physical availability.

Figure C.2 shows the entities involved in the charging interface, i.e. the user, the service provider, and a dishonest party, the last one trying to gain from tampering segments or communications.

As shown in Figure C.2, there are essentially three areas where a dishonest party can gain access, *viz.*:

a) the user's segment (On Board Equipment)

b) the service provider’s segment (Road Side Equipment)

c) the communication between the user's segment and the service provider’s segment

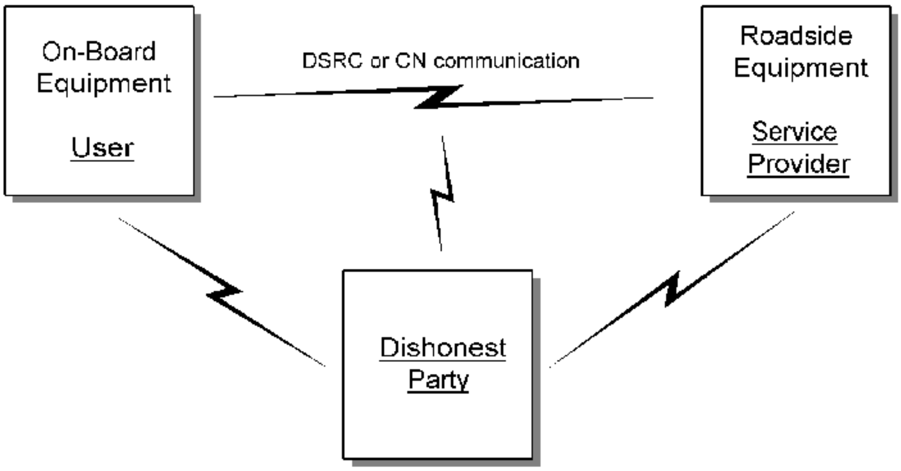


**Figure C.2 — Eavesdropping or breaking into the DSRC communication**

The threats specific to these three areas will be described in the next sections.

### C.5.2 Generic threats to the user’s segment

There are essentially three things a dishonest party can do to the user's segment, *viz*.

a) Segment tampering: tampering with a valid user segment's hardware and associated software and stored data is only possible if physical access to the user segment's hardware (most probably a smart card) is possible, or if modification of a non-valid user segment (e.g. a "blank" smart card) into a valid user segment is an option.

b) Segment impersonation: impersonating the user's segment by mimicking its functionality (the user segment's hardware is not physically compromised here, unlike the first threat).

c) Denial: a dishonest user can deny having used the service supplied. This threat corresponds to a fraudulent user as opposed to a separate dishonest party.

As mentioned, the user's segment most probably will include a smart card (in which case the On Board Equipment is a transparent transponder). It is, however, possible to distribute functionality between a smart card and On Board Equipment which means that the user's segment is made up of two components. Both components would have to adhere to the same security requirements and are handled as one single segment (called On Board Equipment) in this document.

### C.5.3 Generic threats to the service provider’s segment

In analogy with the previous subsection, there are essentially three things a dishonest party can do to the service provider's segment, *viz.*:

a) segment tampering;

b) segment impersonation;

c) denial.

It should be obvious that physical access to the service provider’s centralized equipment will be difficult when compared to the portable/mobile equipment of users. Another difference is the fact that there are not as many service providers as there are users, making service provider's equipment much more controllable, as physical countermeasures will have a much lower impact on total system costs than would be the case with user equipment.

### C.5.4 Generic threats to the communication interface

There are essentially four things a dishonest party can do to the communication interface, *viz*:

a) Eavesdropping: a dishonest party can listen in on communication thus violating the communicating parties' privacy.

b) Manipulation of data communicated in order to gain from it: for example, a dishonest user can try to manipulate charging amounts in an attempt to evade full payment.

c) Replay of data communicated: by replaying messages an attempt could be made to "pay" by means of old payment certificates.

d) Prevention of transmission: can be implemented by sending out a disturbing signal that inhibits any communication. Clearly this is a sabotage action as it is impossible to gain from it. Either the On Board Equipment or the Road Side Equipment can detect the disturbing signal by listening in on the outgoing signal. If this outgoing signal is not equal to what was originally sent, an entry in a log will be made, allowing for later settlement of any disputes. Since the threat “prevention of transmission” will be dealt with procedurally, it will not be included as a threat in the rest of this document.

Due to the nature of communication (notably on the open air interface between On Board Equipment and Road Side Equipment), it is virtually impossible to devise physical countermeasures to detect or prevent attacks aimed at communication. Therefore this kind of threat gets a lot of attention as there is no supplier of hardware or (infrastructure) operator that can be held responsible for attacks at the exchanged information.

### C.5.5 Threats on the charging interface

In Figure C.3 an overview of a full EFC charging transaction is shown.

The communication phases shown are steps within the EFC transaction protocol, which may be physically separated, meaning that each of them, in principle, can be implemented on a separate gantry. It is however possible to combine phases on (preferably) one gantry.

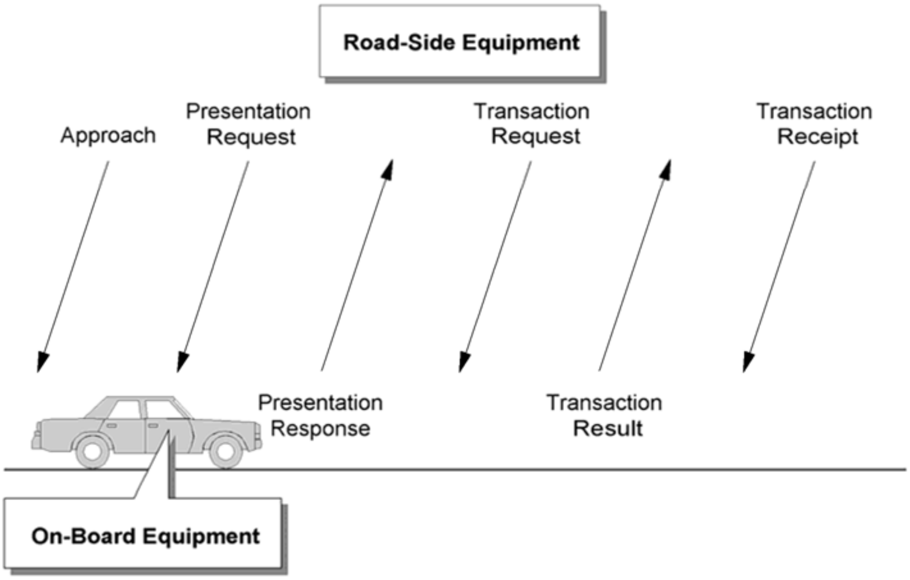


**Figure C.3 — Communication phases in a full EFC charging transaction**

Due to optional phases the content of the transaction in terms of phases may not always be implemented identically, but the sequence of implemented phases is always fixed.

Per communication phase, security services based on threats to the user and the service provider will be described in the next clause.

## C.6 Security services

### C.6.1 General

Security services provide protection against threats. Dependent on the risk factor associated with a threat a security service should have a certain strength. Hence EFC security services should be defined and the different levels of service should be identified. Examples of security services are: authentication services, integrity services, non-repudiation services. The levels of a service are mainly determined by the specific mechanism used.

For all the generic threats we will give a description of the security services required to counter them in Table C.1.

**Table C.1 — Security services needed to counter threats to security**

| Generic threat | Security service | Description of security service |
|---|---|---|
| Segment tampering | Segment integrity | Provides protection against physical tampering of the segment. |
| Segment impersonation | Peer entity authentication | The corroboration that a peer entity in an association is the one claimed. |
| | Data origin authentication | The corroboration that the source of data received is as claimed. |
| Denial | Non-repudiation with proof of origin | The recipient of data is provided with proof of the origin of data. |
| | Non-repudiation with proof of delivery | The sender of data is provided with proof of delivery of data. |
| Eavesdropping | Confidentiality | The property that information is not made available or disclosed to unauthorized individuals, entities or processes. |
| Manipulation | Data integrity | The property that data has not been altered or destroyed in an authorized manner. |
| Replay | Timeliness | Time-dependent information in message including data integrity. |

Authentication (i.e. the security service to counter segment impersonation) is seen to be subdivided in:

— data origin authentication;

— peer entity authentication.

It should be obvious that data origin authentication must be preceded by peer entity authentication as it is otherwise impossible for a receiver to know what cryptographic key(s) should be used for data origin authentication. This observation is based on the premise that authentication makes use of cryptographic algorithms and different segments use different cryptographic key(s) for authentication purposes.

Thus, in the following, data origin authentication and peer entity authentication are taken together and denoted as authentication.

Another observation is that authentication implies data integrity. If authentication did not imply data integrity, it would be possible for a dishonest party to manipulate message contents while leaving authentication-related information intact. The receiver then would conclude, based on authentication-related information, that the message was sent by an authentic segment. This would be incorrect as the message actually was sent by the dishonest party that manipulated its contents.

Summarising this means that:

— ‘data origin authentication’ implies (previous) ‘peer entity authentication’. So in the following only the term “authentication” is used;

— “authentication” implies (simultaneous) “data integrity”.

In the next subclause the notion of "security profile" is introduced linking together the security services needed to counter the threats per communication phase.

### C.6.2 Security profiles

The definition of “security profile” is:

The collection of sensitivity designators (e.g. confidentiality) placed with data such that the data can be secured against threats using security measures.

In principle, a security profile should define the following elements/attributes:

a) the security service(s) [i.e. sensitivity designator(s)] to counter identified threats;

b) the security mechanism(s) and their specific parameters (e.g. key-length when using cryptographic algorithms) to implement the security service(s) with;

c) the data [i.e. specific field(s) in the message] the security mechanism(s) shall be applied to.

In Table C.2, for all communication phases, the security services to counter the threats to user and service provider are summarised. Note that this table is based on Electronic Purse Payment.

Since in this table "segment integrity" is required in all communication phases, it is not considered to be variable and as such is omitted from the table.

**Table C.2 — Security services per communication phase based on threats for Electronic Purse Payment**

| Communication phase | Security services based on threats to the user | Security services based on threats to the service provider |
|---|---|---|
| Approach | — | — |
| Presentation request | — | — |
| Presentation response | Confidentiality | Data integrity<br>Timeliness<br>Authentication |
| Transaction request | Data integrity<br>Timeliness<br>Authentication | Data integrity |
| Transaction result | Confidentiality<br>Non-repudiation | Data integrity<br>Timeliness<br>Authentication<br>Non-repudiation |
| Transaction receipt | Data integrity<br>Timeliness<br>Non-repudiation | Data integrity |

### C.6.3 Security mechanisms

The security services defined in the previous subclause must be implemented by security mechanisms. Note that there are often a number of security mechanisms that can be used to implement a single security service. Table C.3 shows by which security mechanisms certain security services can be implemented (denoted by the shading).

As can be seen from Table C.3, there are several security mechanisms to implement a single security service, and conversely there are several security services that can be implemented by a single security mechanism.

In C.6.4 a description is given of the security mechanisms shown in Table C.3.

**Table C.3 — Security mechanisms used to implement security services**

| Security mechanisms | Security services | | | | | |
|---|---|---|---|---|---|---|
| | Peer entity authentication | Data origin authentication | Data integrity | Timeliness | Confidentiality | Non-repudiation |
| Message authentication code | | | | | | |
| Public key certificate | | | | | | |
| Challenge/response authentication | | | | | | |
| Encipherment | | | | | | |

## C.6.4 Standardization of security mechanisms

### C.6.4.1 Message authentication code

A message authentication code (abbreviated to MAC) can be computed as defined by one of the following International Standards:

— ISO 8731-1[8];

— ISO/IEC 9797-1[9];

— ISO/IEC 10118 (all parts)[11].

Note that any cryptographically strong one-way hash-function can be used to compute a MAC.

Also note that ISO 8731-1 is a subset of ISO/IEC 9797-1. ISO 8731-1 has its foundation in banking, as opposed to ISO/IEC 9797-1 which is a more general International Standard.

These algorithms have in common that the message is used to compute a so-called message digest which is a compact “fingerprint” of the message, similar in concept to a checksum. It represents the message in such a way that if it (the message) were altered in any way, a different message digest would compute from it. This property makes possible detection of any changes to the message.

The second item these algorithms have in common is the fact that during computation of the message digest, or after, encryption is used to make it impossible for entities not having access to the necessary cryptographic key(s) to compute the MAC themselves.

These properties provide two security services as follows.

a) Data origin authentication: it is impossible for entities, not having access to the necessary cryptographic keys (thus they are not authentic, because otherwise they would have access to the necessary keys), to compute a MAC to a message. It is thus possible to authenticate the origin (i.e. the sender) of the message.

b) Data integrity: since it is impossible for entities to change the message's content without the MAC being invalidated, the message's data integrity can be checked by checking the validity of the MAC with the message.

As an example we will discuss MAC computation according to ISO 8731-1.

Computation of a MAC according to ISO 8731-1 makes use of the DES (Data Encryption Standard) encryption algorithm. DES is a symmetric algorithm, which means that both encryption and decryption use the same 56-bit cryptographic key.

More specific, MACs are computed by repeatedly applying DES encryption to 64-bit wide blocks of information which are combined with the 64-bit output blocks of the previous DES encryption. The 32 leftmost bits of the last 64-bit output block of the encryption algorithm are then used as a MAC.

Only authentic senders can compute the MAC correctly since they are the only ones having access to the required cryptographic key(s). Receivers can check this by recomputing the MAC using the cryptographic key(s) corresponding to the sender's (claimed) identity and comparing this recomputed MAC to the MAC added to the message. If both match, assurance that the sender of the message is the one claimed is provided.

Timeliness is not implicitly provided by MACs. If however a timestamp is included in the message, the data integrity property of MACs provides proof that the message, and thus the timestamp, has not been tampered with. A MAC in itself does not protect against replay threats. Adding a timestamp to the message and using a MAC does protect against replay.

#### C.6.4.2 Public Key Certificate

A Public Key Certificate (abbreviated to PKC) computation, using an asymmetric cryptographic algorithm, can be compared to a MAC computation using a symmetric cryptographic algorithm. All properties of MACs also hold true for PKCs.

ISO/IEC 9797-1 and the ISO/IEC 10118 series can be used here, provided that the result from the computation is not truncated. ISO 8731-1 cannot be used since it stipulates the use of the DES symmetric cryptographic algorithm.

The fact that an asymmetric cryptographic algorithm is used however, results – apart from authentication and data integrity – in non-repudiation being offered due to the fact that the key to generate the PKC can be kept secret, and the key to check the PKC (the PKC may not be truncated) can be made public. Entities only having access to public decryption keys can never generate a PKC themselves.

Public Key Certificates are sometimes also called digital signatures.

#### C.6.4.3 Challenge/response authentication

(Peer) Entity authentication is defined in ISO/IEC 9798-4 where it is stated that:

*In the authentication mechanisms specified, an entity to be authenticated corroborates its identity by demonstrating its knowledge of a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check-value. The cryptographic check-value can be checked by anyone knowing the entity's secret authentication key who can recalculate the cryptographic check-value and compare it with the value received.*

By transmitting an identification code as is the case with, e.g., Automatic Vehicle Identification (AVI), it is possible to perform segment identification, but without protection against replay threats. This results from the fact that anyone can record AVI-codes (which in themselves contain no secret information) and replay them at a later time.

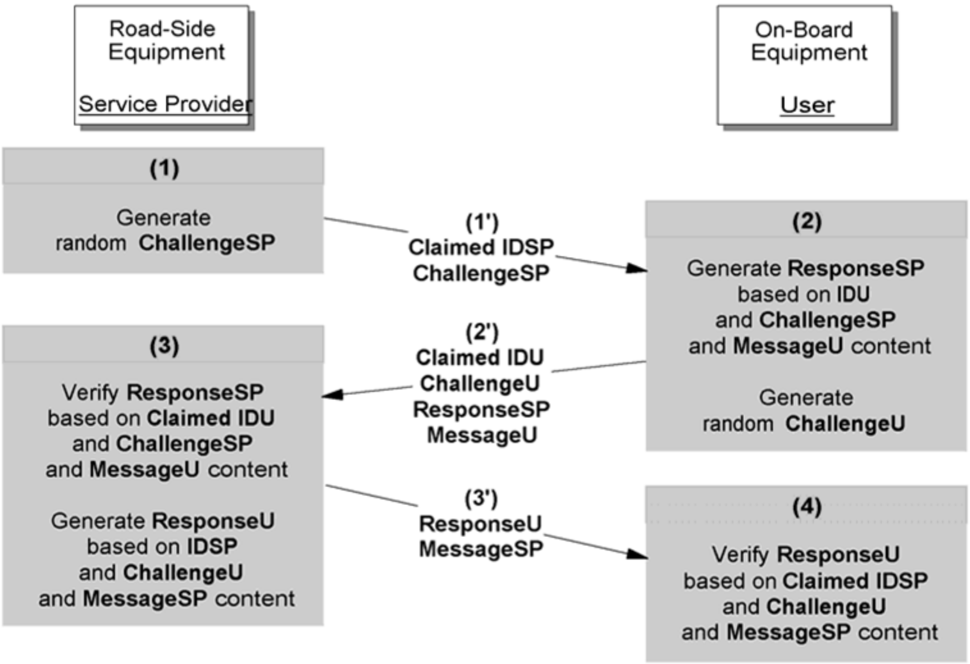
A possible solution to this replay threat is to use a dynamic algorithm instead of the static algorithm used with the AVI-codes.

By using secret information that can be verified by another segment, peer entity- and/or data origin authentication can be implemented.

This dynamic algorithm is called the challenge/response algorithm, an example of which is shown in Figure C.4. Here it is the service provider that initiates the authentication transfer. Both the service provider and the user are authenticated by the other entity.

Note that in Figure C.4 the variables all have “SP” (i.e. service provider) or “U” (i.e. user) added to them. This indicates which entity has initialized that variable. The exception to this rule being the response variables where SP indicates that it is a response to a challenge posed by the service provider. This response is initiated and sent however by the user’s equipment.

In ISO/IEC 9798-4 the authentication transfer shown in Figure C.4 is called mutual three-pass authentication.



Road-Side Equipment
Service Provider
On-Board Equipment
User
(1)
Generate random ChallengeSP
(1')
Claimed IDSP
ChallengeSP
(2)
Generate ResponseSP based on IDU and ChallengeSP and MessageU content
Generate random ChallengeU
(2')
Claimed IDU
ChallengeU
ResponseSP
MessageU
(3)
Verify ResponseSP based on Claimed IDU and ChallengeSP and MessageU content
Generate ResponseU based on IDSP and ChallengeU and MessageSP content
(3')
ResponseU
MessageSP
(4)
Verify ResponseU based on Claimed IDSP and ChallengeU and MessageSP content

**Figure C.4 — Challenge/response authentication shown graphically**

By mutual three-pass authentication, the service provider can check whether the user really is who he claims to be because the user has access to the secret information (cryptographic key) it needs in order to calculate the correct response to the challenge posed by the service provider. The message contents must be included in response computation, because otherwise data integrity (implied by authentication) cannot be guaranteed.

The user can check whether the service provider really is who he claims to be in a manner equivalent to the one described above.

If the secret information is:

- *a symmetric cryptographic key,* then possession of that key implies that the entity to be authenticated is trusted (otherwise he would not have access to the key), thus his claim (of identity) should be trusted. Since however all road-side equipment also has access to that key one can never be quite sure that it was actually the user we want to authenticate that was actually using the key.

- *an asymmetric cryptographic key,* then possession of that key is equivalent to the entity being authentic. Possession of the secret asymmetric key can be verified by decryption of the response using the public asymmetric key corresponding to that secret key. There is only one entity having access to that secret key, thus making authentication based on it very reliable.

Timeliness is included implicitly in the protocol due to the fact that the (random) challenge is different for every communication sequence, thus effectively ruling out replay threats.

### C.6.4.4 Encipherment

In cases where privacy is of concern, the encryption of sensitive information can shield this information from eavesdropping. As opposed to the solutions described above, encipherment encrypts all (or only the sensitive parts of) information found as part of the message instead of encrypting separately computed information (i.e. the so-called hash-value) from the message.

The most well-known cryptographic algorithms that can be used are:

- DEA: Data Encryption Algorithm (also called the DES – Data Encryption Standard); this is a symmetric or secret-key algorithm;

- FEAL: Fast Encryption Algorithm; this also is a symmetric or secret-key algorithm developed by the Japanese NTT;

- RSA: Rivest, Shamir and Adleman (the names of the inventors of the algorithm); this is an asymmetric or public-key algorithm.

As opposed to encipherment of only sensitive information it also is possible to encrypt complete messages, thus shielding their complete contents from eavesdropping. This means that negotiation (e.g. on encryption/decryption keys between communicating parties) needs to be performed beforehand. If negotiation is not performed beforehand, sensitive information (e.g. user IDs in order to select the correct encryption/decryption keys) could be disclosed during negotiations in cleartext. Negotiations however could also be performed using a pre-negotiated negotiation key.

Performance of cryptographic algorithms with respect to timing constraints should be considered before implementing complete message encryption solutions.

# Annex D
(informative)

# Common Criteria Recognition Arrangement (CCRA)

## D.1 Overview

In October 1998, after two years of intense negotiations, government organizations from the United States, Canada, France, Germany and the United Kingdom signed a historic mutual recognition arrangement for common criteria-based evaluations. The arrangement, officially known as the "Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security", was a significant step forward for government and industry in the area of IT product and protection profile security evaluations. The partners in the Arrangement share the following objectives in the area of common criteria-based evaluations of IT products and protection profiles:

— to ensure that evaluations of IT products and protection profiles are performed;

— high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;

— to increase the availability of evaluated, security-enhanced IT products and protection profiles for national use;

— to eliminate duplicate evaluations of IT products and protection profiles;

— to continuously improve the efficiency and cost-effectiveness of security evaluations and the certification/validation process for IT products and protection profiles.

The purpose of this Arrangement is to advance those objectives by bringing about a situation in which IT products and protection profiles which earn a common criteria certificate can be procured or used without the need for them to be evaluated and certified/validated again. It seeks to provide grounds for confidence in the reliability of the judgments on which the original certificate was based by declaring that the certification/validation body associated with a participant to the Arrangement shall meet high and consistent standards. The Arrangement specifies the conditions by which each participant will accept or recognise results of IT security evaluations and the associated certifications/validations conducted by other participants and to provide for other related cooperative activities.

A management committee, composed of senior representatives from each signatory's country, has been established to implement the Arrangement and to provide guidance to the respective national schemes conducting evaluation and validation activities. The current signatories to the Arrangement are shown in Clause D.2 and current registered PPs are shown in Clause D.3.

A complete copy of the Common Criteria Recognition Arrangement can be obtained by following the download instructions http://www.commoncriteria.org/registry/ccra-final.html.

## D.2 CCRA participants

The CCRA participants can be obtained by following the download instructions http://www.commoncriteriaportal.org/members.html.

## D.3 Registered Protection Profiles

The registered Protection Profiles can be obtained by following the download instructions http://www.commoncriteriaportal.org/pp.html.

# Bibliography

[1] ISO/IEC TR 15446; *Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets*

[2] ISO 14906, *Road transport and traffic telematics — Electronic fee collection — Application interface definition for dedicated short-range communication*

[3] ISO/TS 17573, *Road Transport and Traffic Telematics — Electronic Fee Collection (EFC) — Systems architecture for vehicle related transport services*

[4] ISO/TS 17575-1, *Road Transport and Traffic Telematics (RTTT) — Electronic Fee Collection (EFC) — Application Interface Definition for Global Navigation Satellite Systems and Cellular Networks (GNSS/CN) — Part 1: Charging*

[5] ISO/TS 17575-2, *Road Transport and Traffic Telematics (RTTT) — Electronic Fee Collection (EFC) — Application Interface Definition for Global Navigation Satellite Systems and Cellular Networks (GNSS/CN) — Part 2: Communication and connections to the lower layers*

[6] ISO/TS 17575-3, *Road Transport and Traffic Telematics (RTTT) — Electronic Fee Collection (EFC) — Application Interface Definition for Global Navigation Satellite Systems and Cellular Networks (GNSS/CN) — Part 3: Provisions for updating on-board equipment (OBE)*

[7] ISO/TS 17575-4, *Road Transport and Traffic Telematics (RTTT) — Electronic Fee Collection (EFC) — Application Interface Definition for Global Navigation Satellite Systems and Cellular Networks (GNSS/CN) — Part 4: Roaming*

[8] ISO 8731-1, *Banking — Approved algorithms for message authentication — Part 1: DEA*

[9] ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[10] ISO/IEC 9798-4, *Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*

[11] ISO/IEC 10118 (parts 1 to 4), *Information technology — Security techniques — Hash-functions*

## Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

## Copyright

## Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: TED 28 (0978).

### Amendments Issued Since Publication

| Amendment No. | Date of Issue | Text Affected |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

BUREAU OF INDIAN STANDARDS

**Headquarters:**

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
*Telephones*: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.org.in

| **Regional Offices:** | | *Telephones* |
|---|---|---|
| Central : | Manak Bhavan, 9 Bahadur Shah Zafar Marg<br>NEW DELHI 110002 | 2323 7617<br>2323 3841 |
| Eastern : | 1/14, C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi<br>KOLKATA 700054 | 2337 8499, 2337 8561<br>2337 8626, 2337 9120 |
| Northern : | SCO 335-336, Sector 34-A, CHANDIGARH 160022 | 260 3843<br>260 9285 |
| Southern : | C.I.T. Campus, IV Cross Road, CHENNAI 600113 | 2254 1216, 2254 1442<br>2254 2519, 2254 2315 |
| Western : | Manakalaya, E9 MIDC, Marol, Andheri (East)<br>MUMBAI 400093 | 2832 9295, 2832 7858<br>2832 7891, 2832 7892 |

**Branches:** AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi