TECHNICAL SPECIFICATION

ISO/TS 17574

First edition
2004-11-01

Road transport and traffic telematics — Electronic fee collection (EFC) — Guidelines for EFC security protection profiles

Transports routiers et télématique routière — Systèmes de péage électronique — Lignes directrices concernant les profils de protection de la sécurité des péages

Reference number
ISO/TS 17574:2004(E)

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

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

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

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

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

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

An ISO/PAS or ISO/TS is reviewed after three years with a view to deciding whether it should be confirmed for a further three years, revised to become an International Standard, or withdrawn. In the case of a confirmed ISO/PAS or ISO/TS, it is reviewed again after six years at which time it has to be either transposed into an International Standard or withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 17574:2004 was prepared by the European Committee for Standardization (CEN) in collaboration with Technical Committee ISO/TC 204, *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Contents

page

Foreword

This document was prepared by Technical Committee CEN/TC 278, “Road Transport and Traffic Telematics” in collaboration with ISO/TC 204 “Transport information and control systems”.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification : Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Introduction

Electronic Fee Collection systems are subject to several ways of fraud both by users and operators but also from people outside the system. These security threats have to be met by different types of security measures including security requirements specifications. This document provides a **guideline** for preparation and evaluation of security requirements specifications, referred to as Protection Profiles (PP) in ISO/IEC 15408 *Information technology - Security techniques - Evaluation criteria for IT security* and ISO/IEC PDTR 15446 *Guide for the production of protection profiles and security target*. 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 document should be read in conjunction with the underlying standards ISO/IEC 15408 and ISO/IEC PDTR 15446. Although a layman can read the first part of the document to have an overview on how to prepare a Protection Profile for EFC equipment, the Annexes, and more particularly Clauses A.4 and A.5, require that the reader is familiar with the ISO/IEC 15408.

It is recommended that Electronic Fee Collection (EFC) operators or national organisations, e.g. Highway authorities or Transport Ministries, use this guideline to prepare their own EFC/PP, as security requirements should be described from the standpoint of the operators and/or operators organisations.

It should be noted that this standard is of a more **informative** than normative nature and it can not be used without also using the ISO/IEC 15408. Most of the content of the standard is an example shown in Annex A on how to prepare the security requirements for EFC equipment, in this case an OBE with an IC-card loaded with crucial data needed for the EFC. The example refers to a Japanese national EFC system and should only be regarded and used as **an example**. The Clauses 1 to 5 are normative while Annexes A to D are informative.

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

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

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

1 Scope

This document gives **guidelines** for the preparation and evaluation of security requirements specifications, referred to as Protection Profiles (PP) in ISO/IEC 15408 Evaluation criteria for IT security and ISO/IEC PDTR 15446 Guide for the production of protection profiles and security target. By a **Protection Profile** (PP) is meant a set of security requirements for a category of products or systems which meet specific needs. A typical example would be a PP for OBEs to be used in an EFC system and in this case the PP would be an implementation-independent set of security requirements for the OBEs meeting the operators and users needs for security.

The document uses an OBE with an integrated circuit(s) card (ICC) as an example describing both the structure of the PP as well as the proposed content.

Figure 1 shows how this document fits in the overall picture of EFC security architecture. The shaded boxes are the aspects mostly related to the preparation of PPs for EFC systems.

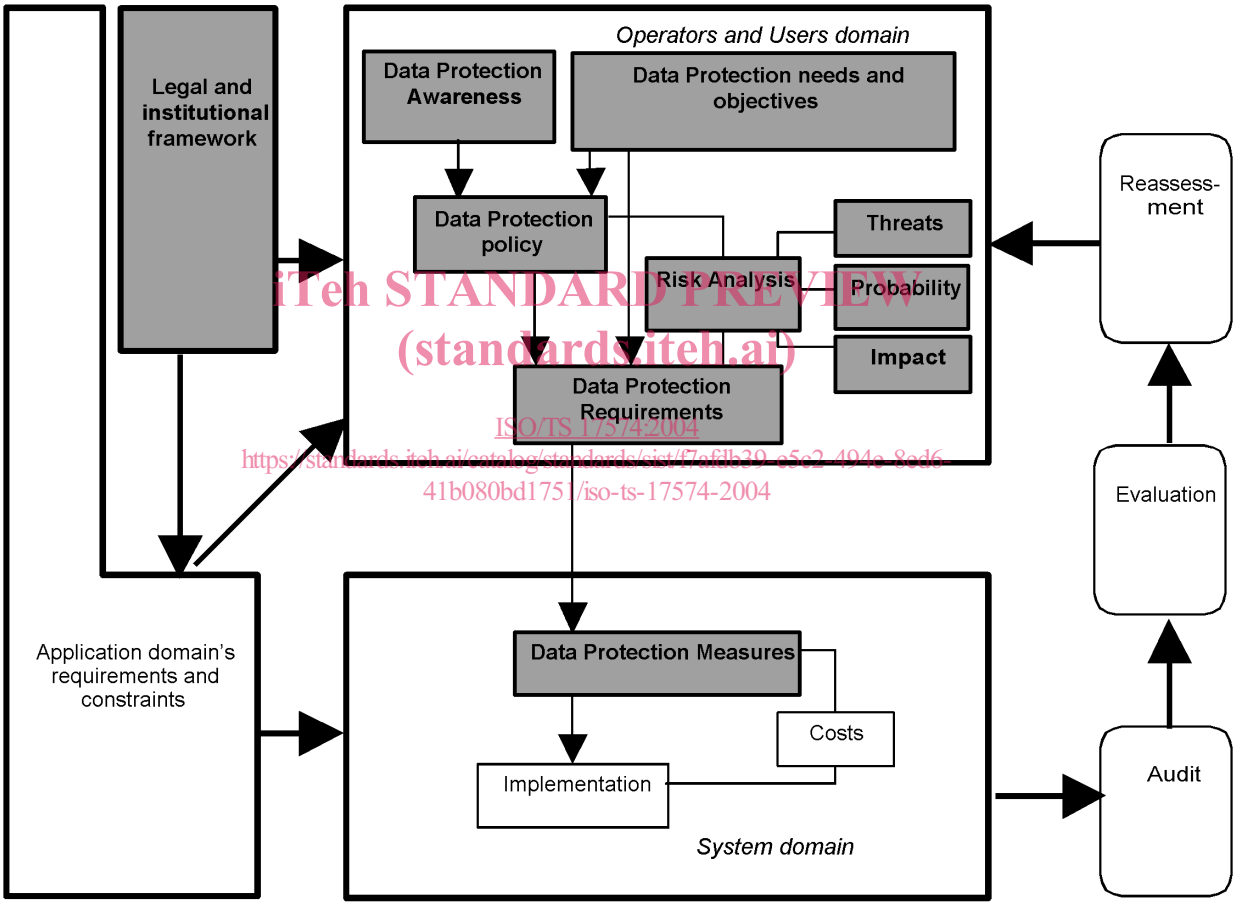

Figure 1 — Overall view of security architecture

The main purpose of a PP is to analyse the security environment of a subject and then to specify the requirements meeting the threats being 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 (items 1 to 6):

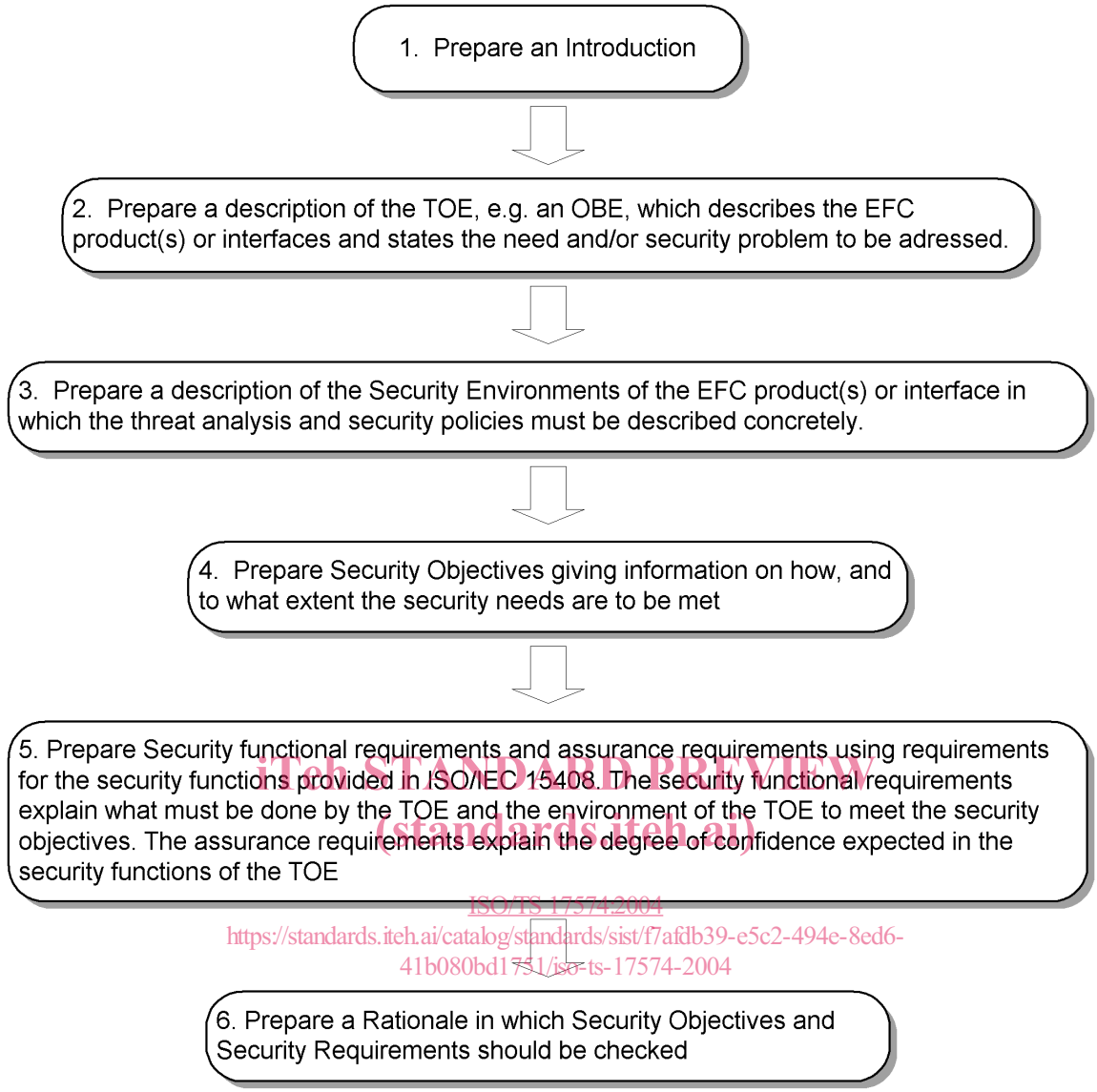

Figure 2 — The process of preparing a Protection Profile for EFC equipment

A PP can be registered publicly by the entity preparing the PP in order to make it known and available to other parties that can 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 can be looked upon as the EFC operator requirements the ST can 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. As for international registry organisation, i.e. Common Criteria Recognition Arrangement (CCRA) and current registered PPs, reference is made to Annex D.

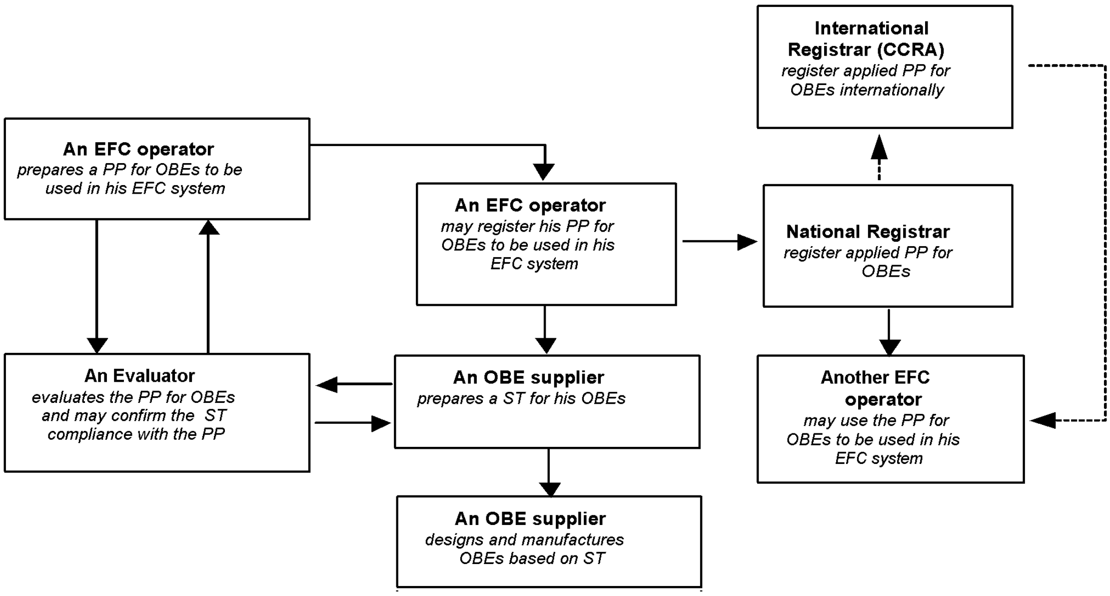

Figure 3 — Relationships between operators, suppliers and evaluators

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

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

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

— finally the rational contains additional evidence establishing that the TOE summary specifications ensures 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.

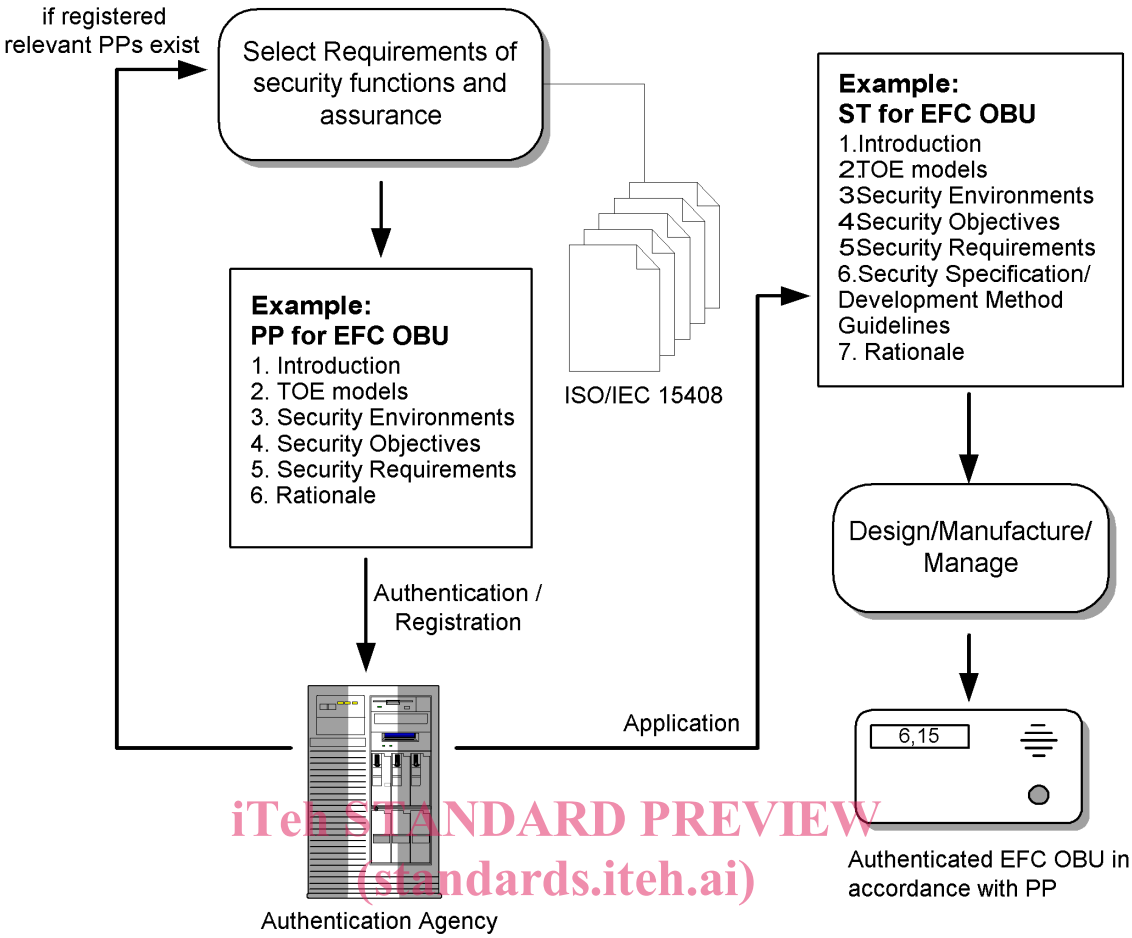

Figure 4 — Example on design based on a PP

TOE for EFC is limited to EFC specific entities and interfaces such as for Users, Service Providers and communication link (DSRC or CN) between Users and Service Providers, which are essential to EFC systems and are shown shadowed in Figure 5. Since the existing financial security standards and criteria are applicable to other entities and interfaces, they are assumed to be outside the scope of TOE for EFC.

The security evaluation is performed by assessing the security related properties of 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 document.

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

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 in this Annex (between the OBE and the RSE) is based on DSRC.

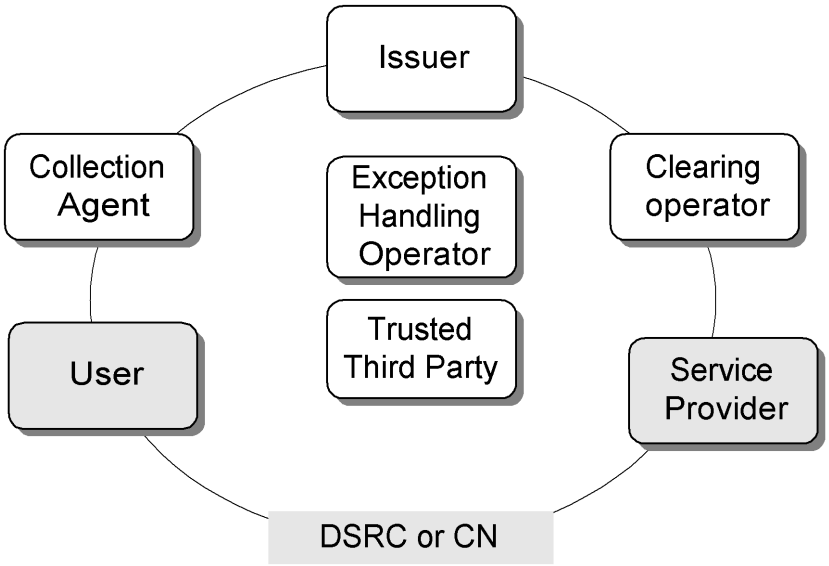

Figure 5 — Scope of TOE for EFC

Figure 6 below shows the entities involved in the charging interface, i.e. the User, the Service Provider, and a Dishonest Party, the latter trying to gain from tampering segments or communication.

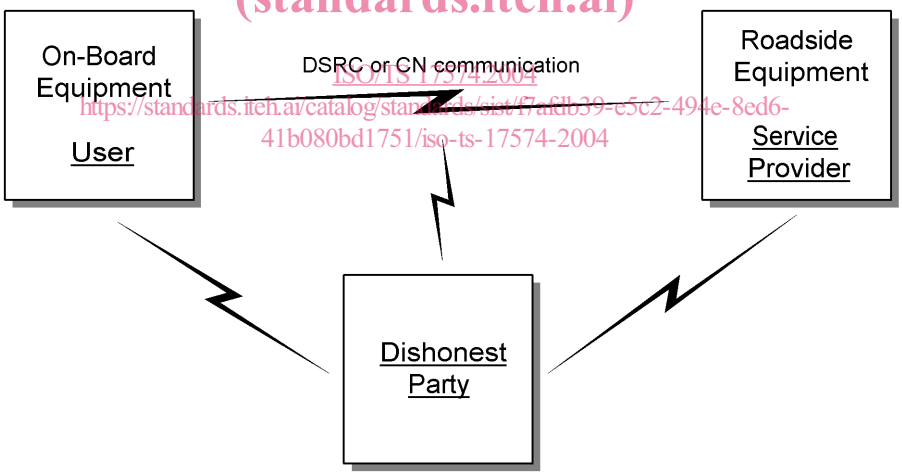

Figure 6 — Entities involved in the Charging Interface of EFC

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 15408-1:1999, *Information technology - Security techniques - Evaluation criteria for IT security – Part 1: Introduction and general model*

ISO/IEC 15408-2:1999, *Information technology - Security techniques - Evaluation criteria for IT security – Part 2: Security functional requirements*

ISO/IEC 15408-3:1999, *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. In addition, 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. 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 OBU

3.5
Central Equipment
system components at fixed centralised 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 is provided that a duly identified product, process or service is in conformity with a specific standard or other normative document

3.7
Clearing Operator
the entity that collects and possibly aggregates transactions from one or more Transport Service Providers for delivery to the Issuer(s). The Clearing Operator can also handle the Apportionment between the Transport Service Providers. In the financial world this operator is equivalent to an Acquirer

3.8
Collection Agent
the entity responsible for selling, reloading or delivering the Payment Means to the User and collecting the payment from the User on behalf of the Issuer. The Collection Agent can also collect user related application specific data from the User. The Collection Agent is also referred to as Retailer

3.9
confidentiality
prevention of information leakage to non-authenticated individuals, parties and/or processes

3.10
Evaluation Assurance Level (EAL)
assurance levels to evaluate securities for products and systems

3.11
functional requirement
security requirements to determine the security functions, which are required for systems and/or products

3.12
issuer
the entity responsible for the payment system and responsible for issuing the Payment Means to the User

3.13
integrity
the property that information (data) has not been altered or destroyed in an unauthorised manner

3.14
Key Management (Encryption Key Control)
the generation, distribution, storage, application and deletion of encryption keys

3.15
On-Board Equipment (OBE)
equipment located within the vehicle and supporting the information exchange with the Road Side Unit or the Central Communication Unit. It is composed of the On-Board Unit and other sub-units whose presence have to be considered optional for the exception of a Transaction

3.16
On-Board Unit (OBU)
minimum component of an On-Board Equipment, whose functionality always includes at least the support of the DSRC interface or/and the Central Communication Unit and the protection of the data stored in the OBU

3.17
operator
generic term for the entities: Issuer, Clearing Operator, Collection Agent and Service Provider

3.18
Personalisation card (Set-up card)
an IC card to transcribe individual data such as vehicle information into an On-Board unit

3.19
privacy
the right of individuals to control or influence what information related to them can be collected and stored and by whom and to whom that information may be disclosed

3.20
protection
the act of protecting, or the state of being protected; preservation from loss, theft, damage or unauthorised access

3.21
rationale (verification)
a process determining that a product of each phase of the system life cycle development process fulfils all the requirements specified in the previous phase

3.22
reliability
An attribute of any system that consistently produces the same results, preferably meeting or exceeding its specifications

3.23
responsibility
the state of being responsible, accountable, or answerable, as for an entity, function, system, security service or obligation

3.24
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

3.25
Secure Application Module (SAM)
a module intended to contain algorithm(s), related keys, security procedures and information to protect an application in such a way that unauthorised access is not possible. This can be achieved through physically, electrically and logically protection of the module

3.26
Security Policy
a set of rules that regulate how to cope with security threats or what degree of security levels should be kept

3.27
Security Threat
a potential action or manner to violate security systems

3.28
Security Target (ST)
a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

3.29
Service Provider
the person, company, authority or abstract entity offering a transport service to the User for which the user has to pay a fee (the fee will in some cases be zero, e.g. emergency vehicles)

3.30
Target Of Evaluation (TOE)
information security product or system for the subject of security evaluation

3.31
User
the entity that uses services provided by the Service Provider according to the terms of the Contract expressed by the Payment Means. The User receives and reloads the electronic Payment Means through the Collection Agent

3.32
validity
the quality or state of being valid; having legal force