PD CEN/TR 16690:2014

BSI Standards Publication

# Electronic fee collection — Guidelines for EFC applications based on in-vehicle ITS stations

...making excellence a habit.™

## National foreword

This Published Document is the UK implementation of CEN/TR 16690:2014.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.


Published by BSI Standards Limited 2014

ISBN 978 0 580 84414 0
ICS 35.240.60

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2014.

### Amendments/corrigenda issued since publication

| Date | Text affected |
|---|---|

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

**CEN/TR 16690**

July 2014

ICS 35.240.60

English Version

# Electronic fee collection - Guidelines for EFC applications based on in-vehicle ITS stations

Perception de télépéage - Lignes directrices pour les applications de télépéage installées dans les stations de systèmes de transport intelligents (ITS) embarquées dans les véhicules

Elektronische Gebührenerhebung - Richtlinien für Anwendungen der Elektronischen Gebührenerhebung basierend auf fahrzeuginternen IVS Geräten

This Technical Report was approved by CEN on 10 May 2014. It has been drawn up by the Technical Committee CEN/TC 278.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels**

# Contents

Page

# Foreword

This document (CEN/TR 16690:2014) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

A CEN Technical Report is a document adopted by CEN/CENELEC containing informative material not suitable for publication as a European Standard or a Technical Specification.

This document has been prepared by CEN/TC 278/WG 1, Project Team 136. The work done by the project team has been governed by the Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN, and by CEN/TC 278/WG 1, Electronic fee collection and access control (EFC).

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

# Introduction

Increasingly, tolling systems are becoming automated and electronic fee collection (EFC) is becoming a pervasive service in Europe. The widespread deployment of EFC systems requires provisions to allow users to employ a single contract and a single OBE to circulate through many different toll domains. In Europe, for example, this need has been officially recognized and legislation on interoperability has already been adopted in the form of the Interoperability Directive 2004/52/EC and the EETS Decision 2009/750/EC.

Standardization in the context of Electronic Fee Collection has been active since the early '90s with the aim of providing the architecture and the definition of interoperable interfaces for interoperable tolling systems. Interoperable interfaces allow tolling systems to exchange information and make mutual use of it. Specifications of such interfaces have been provided in the form of Application Interface Definitions, which are to be considered as toolboxes for defining application protocols and application data exchanged. In many cases, interoperable application profiles have been defined to narrow down the options and provide a sound basis for interoperability.

The standardization results have major relevance for the future of the EETS. Some standards are directly referenced by the EETS Decision and are hence of mandatory application. Other standards provide open and interoperable definitions which are likely to be employed to fulfil the requirement that: “EETS equipment shall be designed in such a manner that its interoperability constituents utilise open standards”.

EFC is one of the intelligent transport systems (ITS) applications with the widest deployment. Currently EFC equipment is mostly dedicated to one or a few applications only. On the one hand, EFC equipment is also becoming more capable and EFC OBE may provide platforms for delivering selected Value Added Services as analysed in CEN/TR 16219. On the other hand, future ITS Stations may in principle deliver the EFC Service to users, if certain requirements are fulfilled.

This Technical Report mainly provides a view on how “both worlds”, the established and wide-spread EFC services and the emerging ITS services and platforms, could be combined to future solutions in which EFC services are considered as one service amongst others offered by ITS. The Report provides information to designers of ITS about the nature and specialities in the EFC services to be taken into account. It also provides EFC stakeholders with guidance how an integration of EFC into the set of services provided in the ITS environment may be achieved.

In order to identify the guidelines how EFC applications can be provided on ITS in-vehicle stations, the following approach is chosen:

— provide a view and understanding of both EFC and cooperative ITS in terms of available architectures, definitions, specifications, stakeholders and operational experiences (commercially available projects as well as research and trial activities);

— identify major EFC requirements that will have an impact to the ITS Station;

— provide a view as to how EFC roles and functionalities (according to ISO 17573) shall be enabled and supported in the cooperative ITS context (in different phases of the entire life cycle of an EFC service);

— identify a base technical architecture that enables EFC services in an ITS context;

— analyse stakeholders in a business architecture and provide an example of a business architecture for EFC services in an ITS environment; and

— emphasize on particular key areas like conformance and certification, potential synergies in the context of the ITS Station, areas of major concern, governance, critical elements.

This approach could be chosen as the EFC environment is seen very mature in terms of architectural, technical and operational requirements and processes. EFC as a service is already in use in various commercial projects in many countries throughout the world. Operational experiences have already been taken into account in refining the landscape of existing specifications in EFC. This can be seen as an extraordinary condition compared to other (future) ITS services for which such mature environmental and context is not yet available

ETSI TC ITS has defined a Basic Set of Applications in ETSI/TR 102 638 which is expected to be deployed relatively swiftly after completion of standardization of C-ITS. EFC is directly addressed in this Basic Set of Applications and considered as a primary application. Standardization of the EFC application requirements is, however, within the scope of CEN/TC 278/WG 1, which is in charge of defining the requirements for the EFC use cases in accordance with the set of standards developed by this Working Group.

# 1 Scope

This Technical Report (TR) contains an analysis of the technical and operational feasibility of using a generic ITS Station as specified in ETSI EN 302 665, *Intelligent Transport Systems (ITS); Communications Architecture*, for EFC applications compliant to the requirements specified in ISO 17573, EN ISO 12855, CEN ISO/TS 17575 (all parts), EN ISO 14906, EN 15509, CEN ISO/TS 12813, CEN ISO/TS 13141 and CEN/TS 16439.

The scope of this Technical Report includes:

— description of the context of Cooperative ITS and the ITS Stations;

— providing details of the context of EFC applications;

— outlining the basic architectural concepts and role model of both EFC and Cooperative ITS;

— identification of core requirement areas for operation of an EFC application on an ITS Station;

— specification of a set of recommendations for functional, operational and security requirements to the ITS Station supporting the EFC application(s);

— description of a possible role model in which the roles known in EFC applications make use of the roles in the C-ITS system in order to provide EFC services in an C-ITS context;

— provision of considerations in particular areas of EFC like certification and governances;

— guideless and recommendations for further standardization work in this area;

— emphasizing on security related elements of EFC that need to be considered in a C-ITS environment.

The scope of this Technical Report is limited to in-vehicle ITS Stations. However, an EFC service always requires the involvement of in-vehicle and central functionalities. Furthermore, for enforcement purposes as well as in DSRC based toll domains for toll charging purposes also, it is essential that road-side based functions are provided and operated. In order to facilitate EFC services a set of functionalities, tasks and responsibilities are defined and specified in an EFC role model (ISO 17573). These functionalities, tasks and responsibilities are shared between the roles Toll Charger, Toll Service Provider, Road User and Interoperability Management. All these roles interact with each other. As a consequence this Technical Report provides in various areas explanations that are beyond the in-vehicle environment. This is required in order to present the full environment and context. It keeps the readability of this document at a sound level and provides valuable information to those readers which are not yet familiar with EFC in detail.

Outside the scope of this Technical Report is:

— detailed technical specifications for EFC services and applications on C-ITS systems;

— implementation specific elements.

# 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 15509, *Road transport and traffic telematics - Electronic fee collection - Interoperability application profile for DSRC*

CEN ISO/TS 12813, *Electronic fee collection - Compliance check communication for autonomous systems (ISO/TS 12813)*

EN ISO 12855:2012, *Electronic fee collection - Information exchange between service provision and toll charging (ISO 12855:2012)*

CEN ISO/TS 13141, *Electronic fee collection - Localisation augmentation communication for autonomous systems (ISO/TS 13141)*

EN ISO 14906, *Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906)*

CEN ISO/TS 17575-1:2010, *Electronic fee collection - Application interface definition for autonomous systems - Part 1: Charging (ISO/TS 17575-1:2010)*

CEN ISO/TS 17575-2, *Electronic fee collection - Application interface definition for autonomous systems - Part 2: Communication and connection to the lower layers (ISO/TS 17575-2)*

CEN ISO/TS 17575-3:2011, *Electronic fee collection - Application interface definition for autonomous systems - Part 3: Context data (ISO/TS 17575-3:2011)*

CEN ISO/TS 17575-4:2011, *Electronic fee collection - Application interface definition for autonomous systems - Part 4: Roaming (ISO/TS 17575-4:2011)*

ISO 17573:2010, *Electronic fee collection — Systems architecture for vehicle-related tolling*

## 3 Terms and definitions

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

**3.1**
**back end**
computing and communication facilities of an actor (e.g. a Toll Charger or a Toll Service Provider) exchanging data with a Front or Back End

**3.2**
**back office**
generic name for the centrally located computing and communication facilities (of a role involved in EFC)

**3.3**
**charge report**
information containing road usage and related information originated at the Front End

**3.4**
**cooperative ITS**
subset of the overall ITS that communicates and shares information between ITS Stations to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone systems

[SOURCE: ISO/DTR 17465]

**3.5**
**electronic fee collection**
fee collection by electronic means

**3.6**
**front end**
part(s) of the toll system where road usage data for an individual road user are collected, processed and delivered to the Back End

Note 1 to entry: The Front End comprises the on-board equipment and an optional proxy.

[SOURCE: CEN ISO/TS 17575-1:2010, 3.13]

**3.7**
**interoperability management**
role that manages the toll charging environment, i.e. defining and maintaining a set of rules that, taken together, defines the policy of a given toll regime or of the overall toll charging environment

**3.8**
**ITS application**
association of two or more complementary ITS-S applications

[SOURCE: ETSI EN 302 665 V1.1.1 (2010-09)]

**3.9**
**ITS service**
service provided by an ITS application to the user of ITS

[SOURCE: ETSI EN 302 665 V1.1.1 (2010-09)]

**3.10**
**ITS station**
entity in a communication network that executes ITS-S applications within a bounded, secured, managed domain comprised of an ITS-S facilities layer, ITS-S networking & transport layer, ITS-S access layer, ITS-S management entity and ITS-S security entity

Note 1 to entry: From an abstract point of view, the term “ITS station” refers to a set of functionalities. The term is often used to refer to an instantiation of these functionalities in a physical unit. The appropriate interpretation is clear from the context. The physical instantiation of an ITS-S is named ITS station unit (ITS-SU).

[SOURCE: ISO 21217:2010]

**3.11**
**ITS station service provider**
role that is responsible for procuring an ITS Station (ITS-S), arranging the installation of such ITS-S in vehicles and maintains an ITS-S

Note 1 to entry: This role offers ITS Service providers to host their services on this ITS-S.

**3.12**
**ITS station unit**
implementation of an ITS-S

[SOURCE: ISO 21217:2010]

**3.13**
**on-board equipment**
equipment located on-board a vehicle including nomadic devices with the function of exchanging information with external systems

**3.14**
**policy framework**
role that is responsible for all governing and institutional activities required in the system

[SOURCE: prCEN ISO/TS 17427]

**3.15**
**system management**
role that is responsible to fulfil all required management activities within the system, this especially includes activities supporting the role 'System Operation'

[SOURCE: prCEN ISO/TS 17427]

**3.16**
**system operation**
role that is responsible for the proper execution of the applications that provide the end-to-end service(s)

[SOURCE: prCEN ISO/TS 17427]

**3.17**
**toll charger**
entity which levies toll for the use of vehicles in a toll domain

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

**3.18**
**toll context data**
information defined by the responsible toll charger necessary to establish the toll due for using a vehicle on a particular toll context and to conclude the toll transaction

**3.19**
**toll declaration**
statement to declare the usage of a given EFC service to a toll charger

**3.20**
**toll domain**
area or a part of a road network where a certain toll regime is applied

**3.21**
**toll service provider**
entity providing toll services in one or more toll domains

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

Note 2 to entry: The Toll Service Provider may provide the OBE or may provide only a magnetic card or a smart card to be used with OBE provided by a third party (like a mobile telephone and a SIM card can be obtained from different parties).

Note 3 to entry: The Toll Service Provider is responsible for the operation (functioning) of the OBE with respect to tolling.

**3.22**
**trusted recorder**
logical entity capable of cryptographic functions, used to provide the OBE with security services, including data confidentiality, data integrity, authentication and non-repudiation

## 4 Symbols and abbreviations

For the purpose of this document, the following abbreviations apply throughout the document unless otherwise specified.

| | |
|---|---|
| ANPR | Automatic Number Plate Recognition |
| BSDM | Bounded Secure Management Domain |
| C2C-CC | Car-to-Car Communication Consortium |
| CALM | Communication Architecture for Land Mobiles |
| CALM FAST | CALM network protocol stack |
| C-ITS | Cooperative ITS |
| CMC | Configuration Management Centre |
| CVIS | Cooperative Vehicle Infrastructure Systems |
| CN | Cellular Network |
| DSRC | Dedicated Short Range Communication |
| EAL | Evaluation Assurance Level |
| EC | European Commission |
| ECU | Electronic Control Unit |
| EETS | European Electronic Toll Service |
| EFC | Electronic Fee Collection |
| EGNOS | European Geostationary Navigation Overlay Service |
| ESO | European Standardization Organization(s) |
| ETSI ITS-G5 | Access layer specification for ITS operating in the 5 GHz frequency band (Draft ETSI EN 302 663) |
| ETSI TC ITS | ETSI Technical Committee on ITS |
| EU7FP | 7th framework program (2007 – 2013) of the European Commission |
| FNTP | Fast Networking and Transport layer Protocol |
| GLONASS | Globalnaya Navigatsionnaya Sputnikovaya Sistema (or Global Navigation Satellite System) |
| GNSS | Global Navigation Satellite System |
| GST | Global System for Telematics |
| HGV | Heavy Good Vehicle |
| HMC | Host Management Centre |
| HMI | Human Machine Interfaces |
| I2I | Infrastructure-to-Infrastructure |
| ITS | Intelligent Transport Systems |
| ITS-S | ITS Station |
| ITS-S SP | ITS Station Service Provider |
| ITS-SU | ITS Station Unit |
| KPI | Key Performance Indicator |
| LAC | Localization Augmentation Communication |

| | |
|---|---|
| LDM | Local Dynamic Map |
| OBE | On Board Equipment |
| OEM | Original Equipment Manufacturer |
| OSGi | Open Services Gateway Initiative |
| PC | Personal Computer |
| PKI | Public Key Infrastructure |
| RSE | Road Side Equipment |
| R&TTE | Radio and Telecommunications Terminal Equipment |
| SAM | Secure Application Module |
| SDO | Standardization Developing Organization(s) |
| SLA | Service Level Agreement |
| TC | Toll Charger |
| TD | Toll Domain |
| TEN-T | Trans-European Transport Network |
| TR | Technical Report |
| TS | Technical Specification |
| TSP | Toll Service Provider |
| VAS | Value Added Services |
| V2I | Vehicle-to-Infrastructure |
| V2V | Vehicle-to-Vehicle |
| WLAN | Wireless local area network |

# 5 Context of C-ITS

## 5.1 Definition of C-ITS

### 5.1.1 Introduction

Cooperative System(s) or Cooperative ITS (C-ITS) is being proposed as a new paradigm in ITS, but its exact definition sometimes remains unclear and is not agreed upon by all stakeholders. The most common understanding is that C-ITS involves vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to enhance safety and efficiency of the road transport system. C-ITS is also considered as a mean to get away from the multitude of proprietary stand-alone devices invading the driver environment. The feeling was that it is not sustainable to put a new box with antennas, display, keyboard, etc. for each new application that was going into the car. This is too costly, too unsafe, does not give interoperability, and is just not safe or sustainable from a windshield real estate point of view.

As a consequence ITS has to evolve from “silos” or vertical integration of all functions for each new application, into a new world of sharing common resources where useful and possible.

The definition of what a cooperative system is has proven to be difficult. There are several reasons for this. A major reason is the existence of a plethora of organizations and projects within the field, each deriving their own definition. This can mostly be attributed to historical reasons, but it has also been influenced by turf wars and commercial pressures from actors in existing markets feeling threatened by this new world. The result is that currently several definitions of C-ITS exist.

### 5.1.2 The European Commission basic definition

The most prevalent understanding of C-ITS is the European Commission (EC) definition (as defined in Mandate M/453): "Co-operative systems are ITS systems based on vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I, I2V) and infrastructure-to-infrastructure (I2I) communications for the exchange of information. Co-operative systems have the potential to further increase the benefits of ITS services and applications".

The objective of the mandate from EC is primarily to create benefits in terms of transport efficiency, sustainability, safety and security. To realize these benefits it is necessary to ensure interoperability through standardization. It is also expected that a realization of C-ITS will contribute to the competitiveness objectives of the EU Internal Market.

### 5.1.3 The vehicle active safety viewpoint

A more restricted understanding of C-ITS is the use of 5,9 GHz 802.11p WLAN communications for V2V and V2I links, where the main application is active road traffic safety. The basic idea is that all vehicles broadcast information that will be received by other vehicles at a distance of up to 1 000 m. The typical applications are warnings or active collision avoidance. This is the understanding from many OEMs and authorities involved in the active safety world, such as the Car-to-Car Communications Consortium (C2C-CC, http://www.car-to-car.org/). In addition to V2V communication some safety related use cases employ V2I/I2V communication, e.g. warning of construction sites or maintenance work.

### 5.1.4 The CEN/ETSI/ISO definition

Whereas the EC definition is seen as too generic, the C2C-CC view is often seen as too restrictive both in terms of technology and services. Therefore CEN/ISO and ETSI agreed on another definition in their response to Mandate M/453:

— a co-operative ITS is a subset of the overall ITS that communicates; and

— shares information;

between ITS Stations[1)] (ITS-S) to:

— give advice; or

— facilitate actions;

with the objective of improving:

— safety, sustainability, efficiency and comfort;

beyond the scope of stand-alone systems.

This definition seems to attract the most support at the moment, and it is important to see that it also defines the boundary towards existing, non-cooperative ITS.

ISO/DTR 17465 (all parts) states the following features of C-ITS:

— the sharing of information between any ITS-SU;

— the sharing of information between different applications;

1) ITS Station defined in ETSI EN 302 665/ISO 21217, e.g. units installed in vehicles, at the road side, in traffic control/management centres, in service centres, or hand-held units.

— the sharing of resources (communication, positioning, security…) in an ITS-SU;

— the authorized use of information for purposes other than the original intent;

— the support of multiple ITS applications on an ITS-SU.

Note that an ITS-SU is not restricted to execute cooperative applications. It might also be used as a platform to implement non-cooperative applications. Therefore an ITS-SU can also communicate with sub-systems in the non-cooperative ITS domain, provided that it can trust these sub-systems to provide credible and accurate data within the appropriate security and privacy constraints.

## 5.2 C-ITS role model and business architecture

### 5.2.1 Role model

#### 5.2.1.1 Introduction

The roles and responsibilities in the context of C-ITS are defined in prCEN ISO/TS 17427. In addition the EU7FP project CVIS has defined a role model with associated responsibilities. In both of these definitions the role models also define responsibilities and liabilities in regard to privacy and data protection issues.

#### 5.2.1.2 Role model introduced by ISO

In prCEN ISO/TS 17427 the definition of roles and responsibilities are based on an organizational or enterprise viewpoint as defined in ISO/IEC 10746 (all parts), *Information technology — Open distributed processing*. The roles are separated into external and internal roles, where the internal roles only exists for the purpose of C-ITS, while the external roles are also involved in other activities (non-C-ITS services and applications). The four major roles from prCEN ISO/TS 17427 are shown in Figure 1.

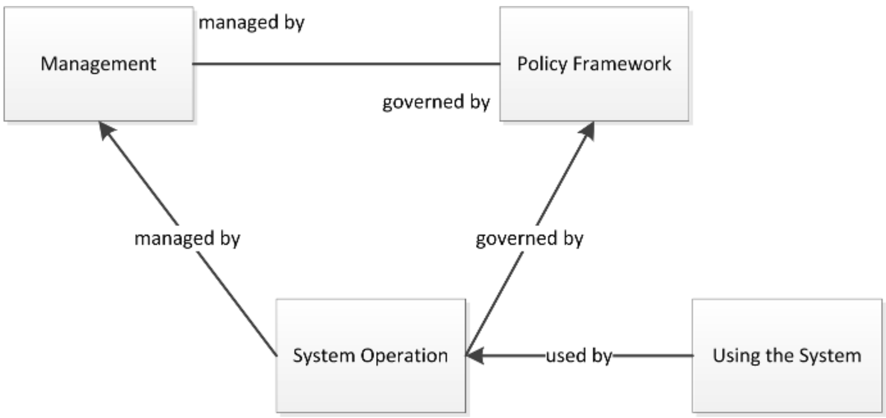



**Figure 1 — Organizational architecture with the four major roles**

The roles System Operation, Management and Policy Framework are further subdivided into sub-roles.

The role System Operation is responsible for the proper execution of the applications that provide the end-to-end service(s). The role System Operation is composed of the sub-roles Content Provision, Service Provision and Presentation Provision. Their general responsibilities are reflected in the process chain shown in Figure 2.

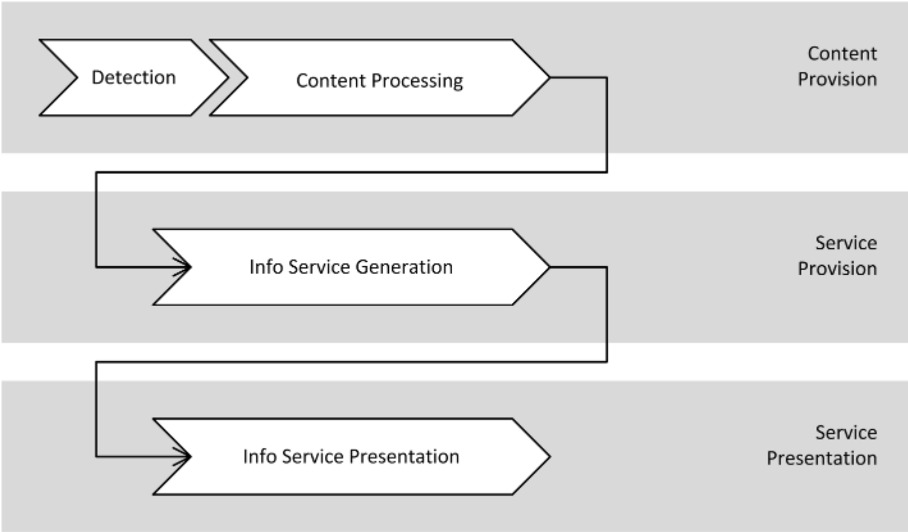



**Figure 2 — Sub-roles of System Operation – process chain**

The role System Management is responsible for all management activities in the system. Sub-roles of System Management are: Service Catalogue Manager, Communication Manager, Service Owner, C-ITS Architect, Project Manager, Test Manager, Service Level Manager, Risk Manager, Capacity Manager, Availability Manager, Information Security Manager, Access Manager, Technical Analyst, Change Manager, Configuration Manager, Homologation Manager, System Monitoring, and optionally Financial Manager.

The role Policy Framework is responsible for all governing and institutional activities in the system and governs the management and system operational activities. Sub-roles of Policy Framework are: Compliance Manager, Policy Institution, Standardization Organization, Security Certificate Body, Legislation/Jurisdiction.

As stated in prCEN ISO/TS 17427 a service might be implemented in multiple ways, each implementation being a possible scenario. A scenario is understood as a transposition of roles to actor groups for the system operation. In addition every implementation scenario additionally deals with System Management and Policy Framework as eminent supporting roles.

Prior to the use of the system each actor needs registration and authorization to request of access permissions. Each role and therefore each actor is responsible to respect both ISO/TR 12859 as well as national regulations and laws on privacy and data protection when participating in C-ITS.

#### 5.2.1.3 Role model developed in the CVIS project

CVIS D.DEPN.3.1, *Design principles for a privacy protective, secure, safe and fault tolerant CVIS design*, describes a role model for C-ITS services. This role model is based on the architecture developed in the GST (Global System for Telematics) project. CVIS has adopted the Reference Model for Open Distributed Processing (RM-ODP) as a structure for its architecture. The role model in CVIS is shown in Figure 3. This role model is based on requirements for privacy, security, safety and fault tolerance.

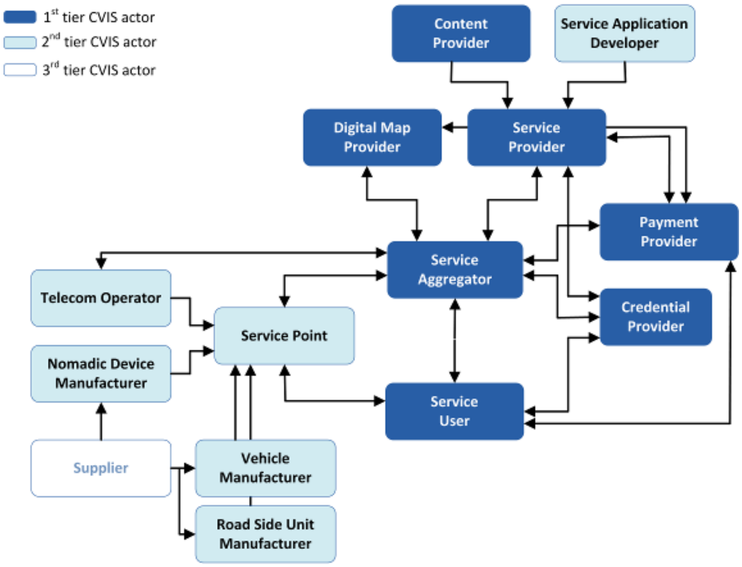



**Figure 3 — CVIS roles [source and courtesy of CVIS]**

### 5.2.2 Business architecture

C-ITS can be considered as a distributed system where there is hardware deployed in vehicles, at the road side, in traffic control/management centres, in service centres, or even as hand-held units. This distributed hardware platform is required to execute services. The hardware platform in itself does not provide value. The software running on the hardware platform provides services, which can generate value. There exists a potential unlimited number of services deployable.

To derive a business architecture all roles and sub-roles as described in previous subclauses need to be assigned to corresponding actors. Where one role can be assigned to multiple actors and one actor can occupy multiple roles. Actors are generally grouped to “vehicle (system)” and “infrastructure (system)”.

In CVIS a conceptual business model template was developed, see Figure 4. This template shows the different actors (grouped in business areas), and enables services to be described as value networks using arrows.

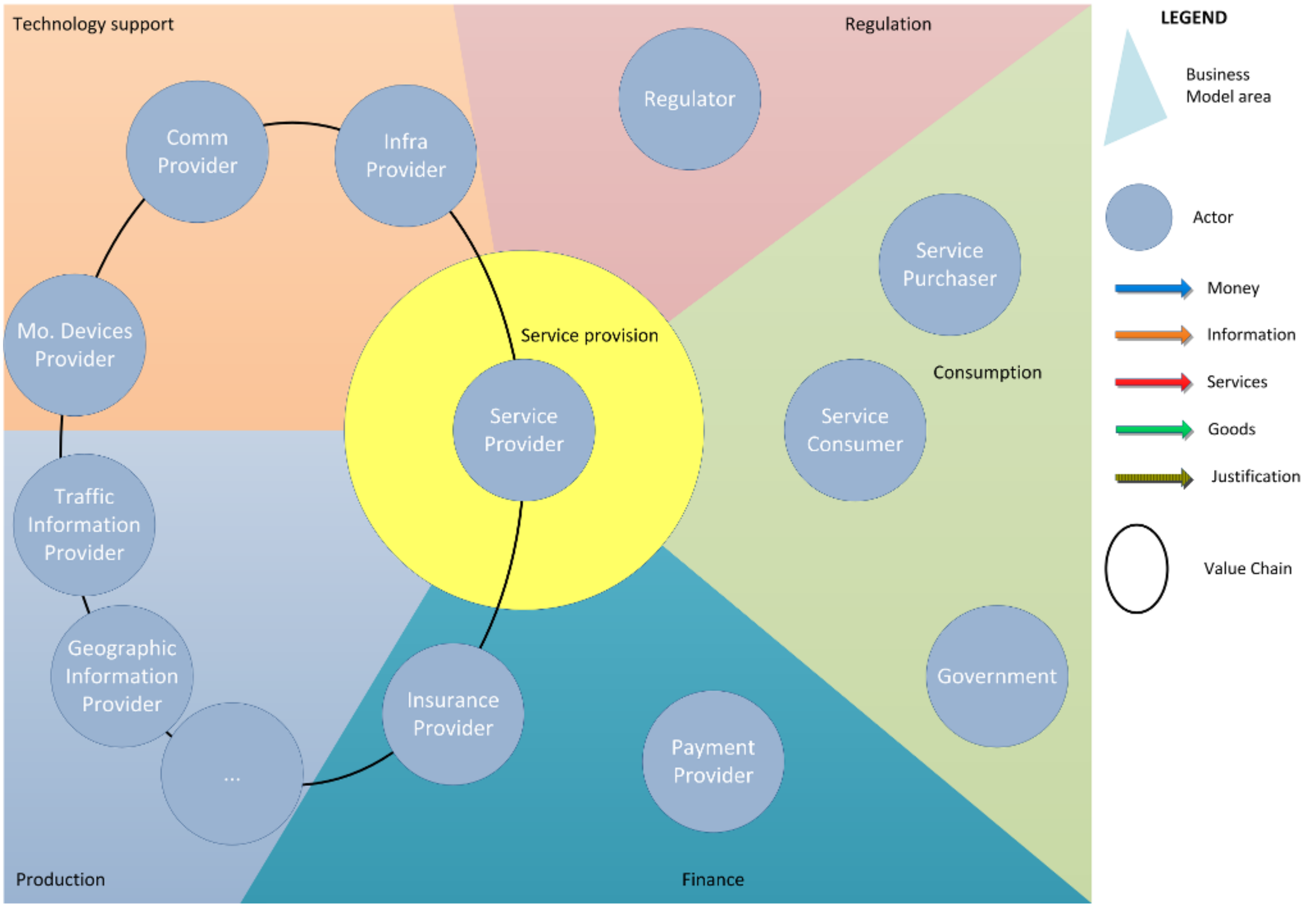



**Figure 4 — Conceptual business model template [source and courtesy of CVIS]**

The different business areas are:

— **Consumption** - This area represents those actor(s) that are perceived as consumers who are paying the service provider for the service(s) delivered to them.

— **Service Provision** - This area represents those actor(s) that are contractually providing the service(s) directly or indirectly through the producers to the consumer(s).

— **Production** - This area represents those actor(s) that are producing the functionality of the service(s) and delivering this functionality to the service provider or directly to the consumer(s).

— **Technology Support** - This area represents those actor(s) that are supporting the producers of the functionality of the service(s) or the service provider with the necessary technology.

— **Finance** - This area represents those actor(s) that are supporting the financial transactions within the business model and the assurances related to the services.

— **Regulation** - This area represents those actor(s) that are monitoring the compliancy with legislation related to the service.

Figure 5 shows an example of a filled-in template. This uses the service “Dangerous goods / route guidance” as an example.

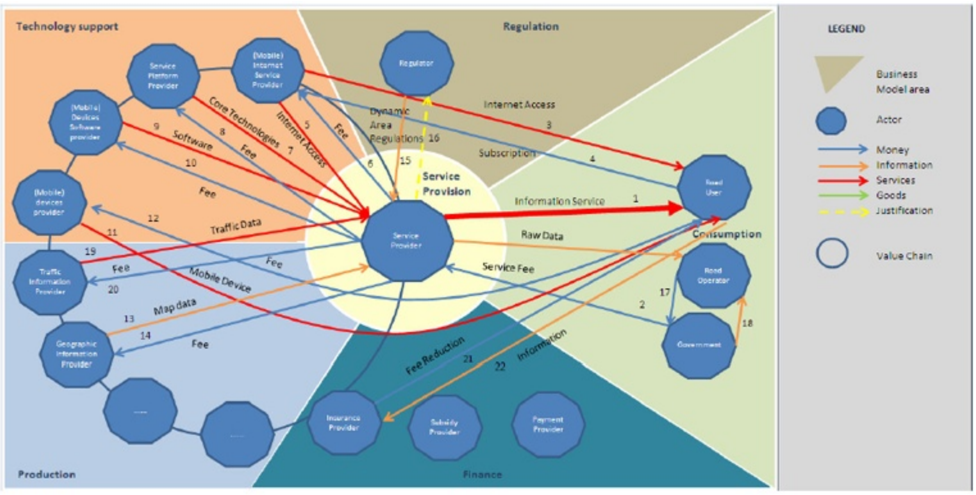



**Figure 5 — The service "Dangerous goods / route guidance" modelled with conceptual business modeller [source and courtesy of CVIS]**

## 5.3 Technical architecture

### 5.3.1 ITS Station architecture

An ITS station (ITS-S) is an important component of the overall ITS communications architecture. The features that most clearly differentiate an ITS-S unit from any other node in the ITS communication network is the station management and security entities that are required. These entities ensure amongst other things the reliability and authenticity that are necessary when deploying safety critical applications and services.

The basic ITS-S reference architecture is shown in Figure 6.

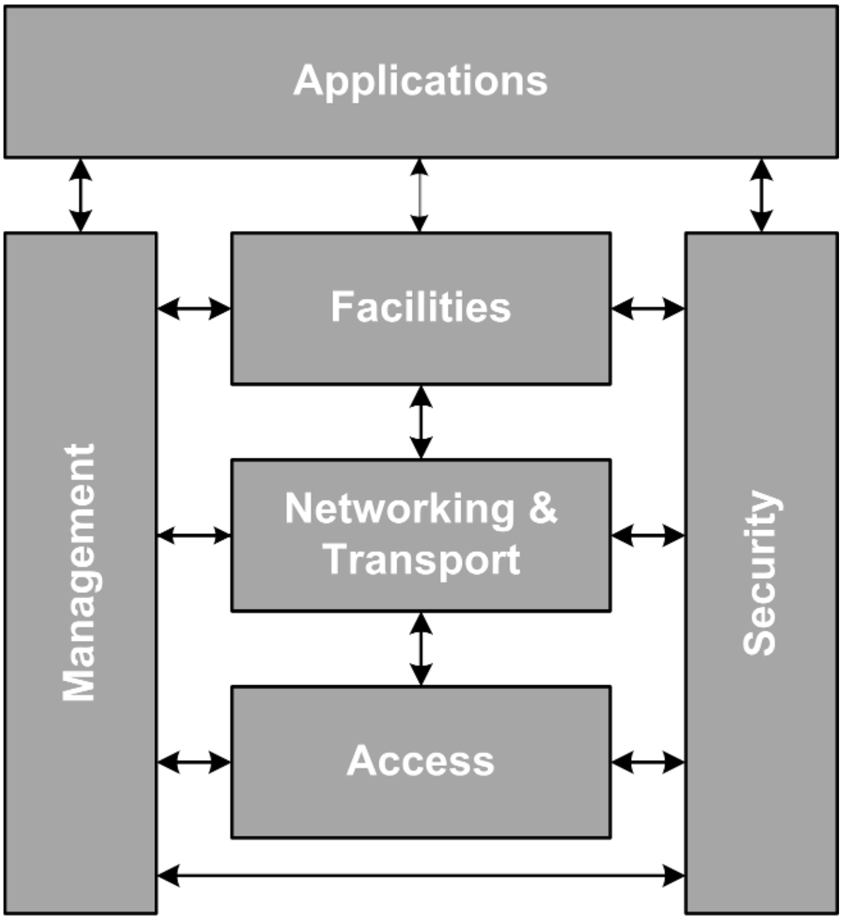



**Figure 6 — Simplified ITS station architecture [source: ISO 21217:2010]**

When a set of such ITS-S are connected together, they form a distributed system and belong to an ITS network. This is described in ISO 21217.

From an abstract point of view, the term “ITS station” refers to a set of functionalities. The physical instantiation of an ITS-S is named ITS station unit (ITS-SU). An ITS-SU may be implemented as one box or as several boxes connected with an ITS station-internal network. A personal ITS-SU might be implemented as a software module inside a smartphone, PDAs or other hand-held device. In larger installations such as in a vehicle, the ITS-SU will often consist of a communications device (Mobile Router) and one or more computers (Mobile Hosts and Gateways to ECUs). For a roadside installation (Roadside ITS-S), there may be several communication devices in an internal network (Access Routers), and several computers running the actual services. In general the following types of ITS-Ss can be identified:

— personal ITS-S (in hand-held devices);

— central ITS-S (part of an central ITS subsystem);

— vehicle ITS-S (in cars, trucks, etc., in motion or parked);

— roadside ITS-S (on gantries, poles, etc.).

### 5.3.2 ITS communication access technologies

The V2I and V2V communication facilities required by C-ITS can be realized using ad hoc short range communication based on wireless local area network (WLAN) technologies. The prevalent standard for this is

IEEE 802.11p. Alternatively, or as a supplement, commercial cellular networks such as 2G/3G and 4G (LTE) can be utilized.

The idea of using WLAN technologies for V2V and V2I has been widely accepted around the world, and in many regions and countries frequency bands around 5,9 GHz has been reserved for this purpose. In Europe the EC has adopted a decision “on the harmonised use of radio spectrum in the 5875-5905 MHz frequency band for safety related applications of Intelligent Transport Systems (ITS)” [2008/671/EC].

The use of ad hoc short range communication enables low latency communication, which is important for safety. It also enables easy and low cost dissemination of localized information to nearby ITS-SUs.

Many use cases for C-ITS require ubiquitous Internet connectivity. This can be realized using commercial cellular networks, but also suitable positioned roadside access points can be utilized.

Several different protocols have been specified to be used in C-ITS. Different protocol exists at each layer (see Figure 6). Some examples are:

a) ITS-S access layer:

   1) IEEE 802.11;

   2) IEEE 1609.4;

   3) ETSI ITS-G5;

   4) M5;

   5) IR (ISO 21214)

   6) GSM;

   7) UMTS;

   8) LTE;

b) ITS networking and transport layer:

   1) IPv4 TCP/UDP;

   2) IPv6 TCP/UDP as specified in ISO 21210;

   3) Fast Networking and Transport Layer Protocol (FNTP - ISO 29281-1);

   4) GeoNetworking Basic Transport Protocol (BTP);

   5) WAVE Short Message Protocol (WSMP);

   NOTE EU/US harmonization task groups HTG1/3 recommended merging the WAVE protocols WSMP/WSA with the ISO protocols FNTP/FSAP.

c) ITS-S facilities layer:

   1) Cooperative Awareness Message (CAM);

   2) Decentralized Environmental Notification Messages (DENM);

   3) Signal Phase and Timing Message (SPaT);

d) ITS-S management entity:

1) FAST Service Advertisement Protocol (FSAP - ISO 24102-5);

2) ITS station internal management communication protocol (IICP - ISO 24102-4).

### 5.3.3 Application provisioning and life cycle management

C-ITS is all about the sharing of information between ITS-S application processes within and amongst ITS stations. In addition C-ITS is also seen by several stakeholders as a mean to get away from the multitude of proprietary stand-alone boxes invading the driver environment. Here the goal is the ITS-SU that will serve as a platform for ITS applications, where the applications share common resources where possible (using the facilities layer shown in Figure 6). It is expected that the set of applications installed on any ITS-SU will change during its lifetime, both due to existing services being improved and new services being invented. As the set of applications is unknown during manufacturing, facilities for service provisioning and life cycle management is most likely needed. Several means to achieve this already exist, but a prevailing view is that each ITS-SU needs to be managed by a configuration management centre (CMC). Such a mechanism was implemented and tested in the CVIS project. The responsibilities of the CMC is both provisioning and remote monitoring. One CMC can serve multiple ITS-SUs. A single ITS-SU may be connected to different CMCs. This is illustrated in Figure 7 and shows the three steps to install new applications:

1) service creation;

2) service deployment; and

3) service provisioning.

The provisioning procedure is responsible, using remote management mechanisms, for life cycle management of the applications. This includes installing, starting, stopping and updating the applications. Note that the service execution step (not shown in the figure), utilizes information exchange between ITS-Ss and/or one or more service centres (central ITS-S).

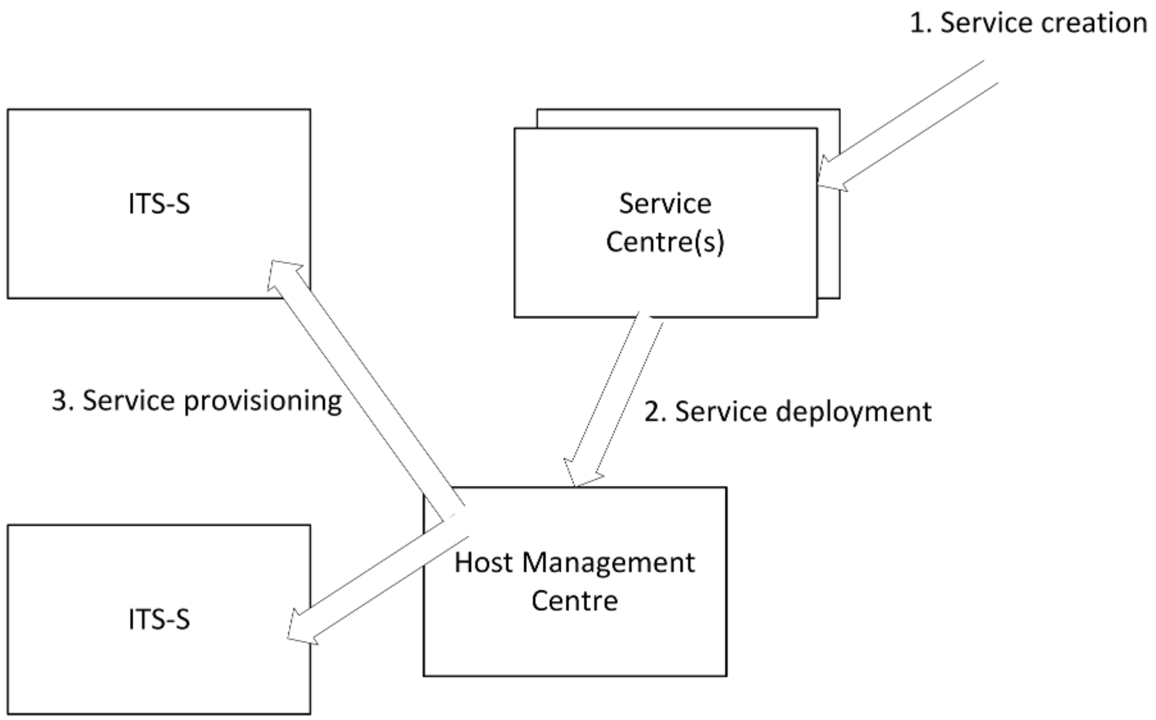



**Figure 7 — Service deployment and provisioning (adapted from CVIS)**

The provisioning of ITS-S applications, ITS-S facilities and ITS-S protocols to an ITS-SU is typically triggered by a subscription request from the user. But it is also possible to deem some applications mandatory. This can for example be applications that are mandatory for an area. Examples of such applications can be of regulatory kind such as electronic fee collection, electronic registration identification and low emission zones.

To enable provisioning and life cycle management a harmonized software run-time platform is needed. Several of the projects described in 5.6 have chosen to use the OSGi framework. The OSGi framework is a module system and service platform for the Java programming language. It implements a dynamic component model and allows applications to be remotely installed, started, stopped, updated, and uninstalled without interfering with the running of other concurrent applications.

#### 5.3.4 Security

In ISO 21217 the ITS-S (as shown in Figure 6) is defined to be within a bounded secured management domain (BSMD). This is a requirement to be able to meet the stringent security requirements of ITS applications related to safety and enables secure peer-to-peer communication between ITS-SUs. The BSMD enables the ITS-SU to be trusted to operate according to the policies and procedures assigned to it by a trusted authority. To establish and maintain this trust there is a need for a public key infrastructure (PKI) for both trust assertion and certificate management.

The ETSI security framework for ITS is a guideline for the secure implementation of ITS applications based on the communication and ITS station architecture defined in ISO 21217 extended by a common security architecture.

ETSI's Specialist Task Force 423[2)] has elaborated a set of ITS security standards. All standards are part of the package *Intelligent Transport Systems (ITS); Security* and deal with a certain aspect:

— ETSI/TS 102 940, *ITS communications security architecture and security management*;

— ETSI/TS 102 941, *Trust and Privacy Management*;

— ETSI/TS 102 942, *Access Control*;

— ETSI/TS 102 943, *Confidentiality services*.

The ITS security package above refers and is based on ETSI/TS 102 731, *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*.

More detailed security considerations are provided in Annex A.

### 5.4 Legal aspects and background

#### 5.4.1 European action plan and directive for ITS

In 2008 the EC published an *Action Plan for the Deployment of Intelligent Transport Systems in Europe* [COM(2008) 886 final]. The purpose of this action plan is to accelerate and coordinate the deployment of ITS throughout Europe, with the final goal of creating benefits in terms of transport efficiency, sustainability, safety and security, while contributing to the EU Internal Market and competitiveness. The action plan outlines six action areas. In action area 4, *Integration of the vehicle into the transport infrastructure*, the development and adoption of an open in-vehicle platform supporting C-ITS is specified. This action area is also the basis for M/453.

The action plan was followed by Directive 2010/40/EU in July 2010 (the ITS directive). The purpose of the directive is the same as the action plan, but a directive is a legislative act which requires member states to

2) ETSI Specialist Task Force 423 received funding in the framework of the ICT Standardisation Work Program of the European Commission.

achieve a particular result without dictating the means of achieving that result. The four first action areas from the action plan maps to the directives four priority areas.

### 5.4.2 User privacy and data protection

The central concept of C-ITS is the communication and sharing of information between actors in the transport system. For several of the new C-ITS applications and services this will involve the communication and processing of personal data. Therefore relevant legislations for user privacy and data protection need to be adhered to when deploying C-ITS.

In the EC *Action Plan for the Deployment of Intelligent Transport Systems in Europe,* action 5.1 is to assess security and data protection aspects related to ITS.

The ITS directive (2010/40/EU) refers to Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector) for the processing of personal data.

### 5.4.3 Liabilities regarding application performance / suitability for use

Liability issues has been identified as a possible barrier to the deployment of C-ITS. These liability issues are related to any technical malfunctions or operational errors that potentially result in injuries and loss of lives due to accidents, loss of money due to inefficiencies, or even loss of privacy due to non-confirming processing of personal data.

In the EC *Action Plan for the Deployment of Intelligent Transport Systems in Europe,* action 5.2 is to address liability issues pertaining to the use of ITS applications and notably in-vehicle safety systems. The ITS directive (2010/40/EU) states that the member states shall ensure that issues related to liabilities relevant for ITS shall be addressed in accordance with European Union law, including in particular Directive 85/374/EEC (on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products).

## 5.5 Overview of standardization activities

### 5.5.1 Introduction

Within ITS standardization there are three Standardization bodies that are of special interest. These are CEN/TC 278, ETSI TC ITS and ISO/TC 204. In addition IEEE also plays an important role in certain aspects of ITS standardization through their 802.11 and 1609 Working Groups. In Europe CEN/TC 278 and ETSI TC ITS are of particular interest since they has special focus on European legislations. To ensure and support a fast work progress and cooperation in standard development the EC has created so called mandates. These shall ensure that standards are developed within certain high focused areas. In 2009, the EC issued mandate M/453 which invited the European Standardization Organisations (ESOs) - CEN, CENELEC and ETSI – to prepare a coherent set of standards, specifications and guidelines to support European Community wide implementation and deployment of Co-operative Intelligent Transport Systems (ITS). CEN and ETSI have formally accepted the Mandate.

CEN and ETSI have agreed to jointly develop the response and work programme under this Mandate with a list of minimum set of standards for interoperability and other identified standards and technical specifications to support Co-operative ITS services. The minimum set of standards is understood as a set of standards which forms the essential basis for the realization of C-ITS and simultaneously is open for extension with regard to applications and as well with regard to other technologies. The work programme also defines an agreed split of responsibility and tasks between CEN and ETSI as well as a detailed description of the on-going cooperation between the two ESOs.

The division of responsibilities is centred on primary capabilities, with the competence of ETSI being in the field of communications and the relation of ETSI to the Car-2-Car Communication Consortium with the experience of vehicle-to-vehicle applications. CEN has a focus on the overall framework architecture and on the roadside and traffic management applications, which mainly involve vehicle-to-road-infrastructure and infrastructure communications.

The ITS Coordination Group (ITS-CG) between CEN and ETSI has been established to ensure on-going coordination of the standardization activities within these two SDOs.

ISO, IEC and ITU are global SDOs who standardize ITS on a global level. Many of the working groups (WGs) with CEN are joint working groups with ISO. To harmonize and obtain a good and fruitful cooperation CEN/TC 278 and ISO/TC 204 has joint meetings twice a year.

ITS standardization is also going on in US, both within IEEE and SAE. An EU-US joint declaration of Intent on Research Cooperation in Cooperative systems has been established.

Cooperation between global ITS SDOs is important in order to achieve harmonized standards providing global interoperability. Detailed cooperation between the SDOs has been initiated in addition to the already existing cross participation by membership in the relevant organisations.

The scope of the standardization activities is broad to cover the complete architectural hierarchy. It covers amongst others:

— standardization of architectures for ITS services;

— various radio communications systems;

— formats and structure of message systems and transport;

— security and privacy technologies and system aspects;

— interfaces and reference points;

— database technologies and data file structures.

The usage areas of the standards can be grouped into categories such as:

— traveller information systems;

— transport control systems;

— vehicle to driver communication (HMI);

— vehicle to vehicle communication;

— vehicle to roadside communication;

— goods and vehicle information;

— public transport aspect including emergency systems.

#### 5.5.2 Basic set of ITS applications

In CEN/ETSI Task Force on Standardization Mandate M/453 1st report, *Programming report under M453*, framing is defined by both a framework architecture and a communication architecture which supports the implementation of a basic set of applications as described in ETSI/TR 102 638. The selection for the basic set of applications was based on an opinion making process with involvement of representatives from key relevant stakeholders

In detail, the following application classes are considered in the minimum set of standards:

— Cooperative Awareness Driving Assistance (safety): Information from other vehicles as basis for the generation of in-vehicle Warnings: Emergency Vehicle Warning, Intersection Collision Warning, Slow Vehicle Warning, Motorcycle Approaching Indication;

— Floating Car Data Collection for Roadside Applications: Collection of Information from vehicles for infrastructure applications;

— Event Driven Road Hazard Warning V2I, I2I: Based on a certain event a warning message is sent out: Roadwork Warning, Wrong Way Driving Warning, Collision Risk Warning from an ITS-S Roadside, Traffic Condition Safety Warning, Weather condition warning;

— Event Driven Road Hazard Warning V2V: Based on a certain event a warning message is sent out: Emergency Electronic Brake Light, Stationary Vehicle Warning, Roadwork Warning, Wrong Way Driving Warning, Traffic Condition Safety Warning, Weather condition warning;

— Traffic Management V2I, I2I: Optimum traffic throughput via speed limits, centrally determined routing, road network management, no overtaking for trucks monitoring and routing of dangerous goods;

— Traffic Management V2V: Improved traffic throughput based on information from other vehicles e.g. position, speed, acceleration information;

— Cooperative Traveller Assistance: Navigation considering information received about restricted access, etc., parking information/booking;

— Value Added Services: Insurance and Financial Services.

The mandate covers the development of a minimum set of standards that allows the implementation of the basic set of applications. This set is extensible, by principle, in order to facilitate a sustainable deployment of the system.

In ETSI/TR 102 638 Electronic Toll Collection is defined as a co-operative traffic management application. The use case defines use of I2V communication to broadcast electronic toll payment capabilities from RSU. ETSI/TR 102 638 also defines two similar use cases; one for automatic access control/parking management and another for local electronic commerce. These two use cases are classified as applications for comfort and entertainment.

### 5.5.3 CEN/TC 278/WG 16 on cooperative systems

CEN/TC 278 is an European standardization body with the name “Intelligent Transport Systems”. CEN/TC 278 was the first ITS standardization body, and CEN/TC 278 has laid the ground works for global ITS standards. In general, CEN has a good representation and participation from industry, service providers, public bodies and road operators/authorities, but less from car makers.

Within CEN/TC 278, Working Group (WG) 16 has the responsibility for standards related to Co-operative systems. As defined in the response to M/453 CEN has a focus on the overall framework architecture and on the roadside and traffic management applications, which mainly involve vehicle-to-road-infrastructure and infrastructure communications.

### 5.5.4 ISO/TC 204/WG 18 on cooperative systems

ISO/TC 204/WG 18 is a joint working group with CEN/TC 278/WG 16.

#### 5.5.5 ISO/TC 204/WG 16 on wide area communications/protocols and interfaces

ISO/TC 204/WG 16 - wide area communications/protocols and interfaces – has defined the CALM (Communication Access for Land Mobiles) set of standards. The goal is to provide ubiquitous continuous communication for ITS services, both between vehicles and between vehicles and the infrastructure. Working Group 16 produced the globally applicable ITS communication architecture (ISO 21217) where different communication protocol stacks are combined, and the actual protocol stack used at any time is dependent on the current availability and capabilities of the protocol stacks and the application requirements and objectives. This “best” choice of available communication protocol stack is transparent to the application (prCEN ISO/TS 17423).

The ITS communication architecture ISO 21217 makes a distinction between *ITS-S specific access technologies,* which have been specifically designed for CALM, and *other access technologies*, which is included in the architecture by an adaption layer. An example of the former is IR (ISO 21214), which specifies the use of infrared light technologies for V2V and V2I communication. Example of the latter are M5 (ISO 21215) and 2G/3G (ISO 21212 and ISO 21213).

In the ITS-S network and transport layer, both standard IPv6 based communication, including NEMO (Network Mobility), and a protocol optimized for low latency V2V and V2I communication called FNTP (Fast Network and Transport Protocol) has been defined (see ISO 21210 and ISO 29281-1).

#### 5.5.6 ETSI Technical Committee on ITS (ETSI TC ITS)

ETSI is the European Telecom Standardization Institute, and is a major contributor to global telecom standards such as GSM and DVB. ETSI does also have a formal and legal role in Europe since it produces Harmonized European Norms, which is an operative part of the R&TTE directive that allows sale and operation of radio equipment without type approval. ETSI is a private institution with paying members.

The stated mission of ETSI Technical Committee ITS is the creation and maintenance of standards and specifications for the use of information and communications technologies in future transport systems. Current focus is mostly on wireless communications for V2V and V2I communications.

The work of ETSI TC ITS is divided in five working groups:

— WG1: User and application requirements;

— WG2: Architecture and cross layer;

— WG3: Transport and network;

— WG4: Medium and medium related;

— WG5: Security.

Together these WGs cover all parts of a protocol stack for V2V and V2I communication. On the application side the focus of ETSI is on road safety. The ITS communication architecture is defined in ETSI EN 302 665, which is based on ISO 21217.

### 5.6 Overview of R&D projects and other relevant initiatives

#### 5.6.1 CVIS project on cooperative vehicle infrastructure systems

CVIS (Cooperative Vehicle Infrastructure Systems) was an integrated R&D project co-funded by EC – DG INFSO, under the ICT priority of the 6th Framework Programme for Research. The project ran from 2006 to 2010. In CVIS a platform for C-ITS was developed. This C-ITS platform, consisting of hardware and software prototypes for in-vehicle and roadside deployment, allows mobile units, roadside units and centres to interact and communicate seamlessly. The CVIS platform features:

— an implementation of the ISO set of standards, including M5 (ISO 21215), IR (ISO 21214), 2G/3G (ISO 21212 and ISO 21213) media;

— a JAVA/OSGi based software and runtime environment supporting application provisioning and life cycle management.

In addition to the platform development CVIS also implemented selected services for increased road efficiency and safety, running on top of this platform.

The CVIS high-level architecture is shown in Figure 8.

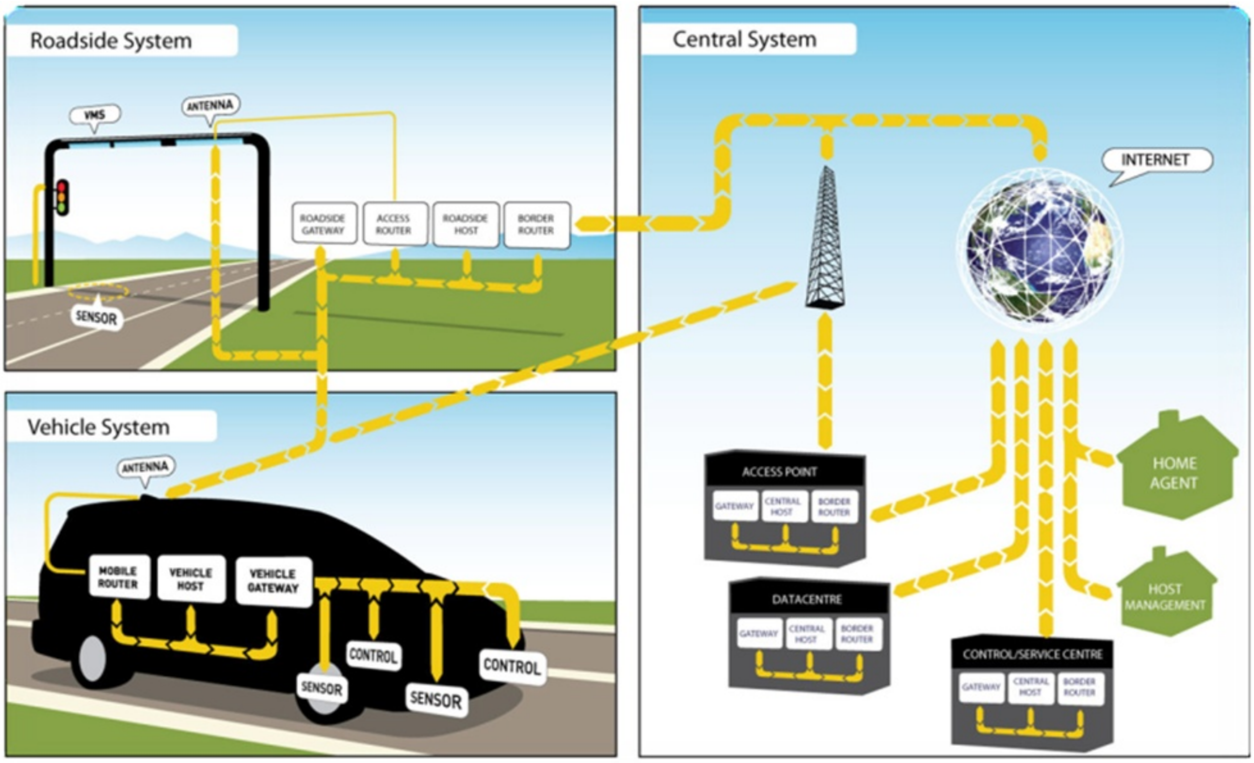



**Figure 8 — CVIS high-level architecture [source and courtesy of CVIS]**

### 5.6.2 SAFESPOT project on road safety related applications

SAFESPOT (Cooperative vehicles and road infrastructure for road safety) was an integrated R&D project co-funded by EC – DG INFSO, under the ICT priority of the 6th Framework Programme for Research. The project ran from 2006 to 2010. The goal of SAFESPOT was based on C-ITS techniques to develop a “safety margin assistant” for drivers. To achieve this several C-ITS prototype applications was developed and tested. Due to cooperation with the CVIS project these prototype applications were also portable to the CVIS platform. Due to the safety focus of SAFESPOT only 802.11p/ M5 based communication technology was employed.

#### 5.6.3 eCoMove project on road transport efficiency applications

eCoMove (Cooperative Mobility Systems and Services for Energy Efficiency) is an integrated R&D project co-funded by the European Commission under the 7th Framework Programme for Research and Development. The project period is from April 2010 to March 2013. The project goal was to create an integrated solution for road transport energy efficiency to help drivers, freight and road operators:

— save unnecessary kilometres driven (optimised routing);

— save fuel (eco-driving support);

— manage traffic more efficiently (optimised network management);

The project’s core concept is that there is theoretical a minimum energy consumption achievable with the “perfect eco-driver” travelling through the “perfectly eco-managed” road network.

The technical platform to implement the eCoMove services is heavily based on the outcome of the CVIS project, including a JAVA/OSGi based software and runtime environment for applications.

#### 5.6.4 DRIVE C2X project with focus on field trials

DRIVE C2X is an integrated R&D project co-funded by the European Commission under the 7th Framework Programme for Research and Development. The project period is from January 2011 to December 2013. The project objectives are:

— carry out a comprehensive assessment of cooperative systems through extensive European field operational tests;

— create and harmonize a European wide testing environment for cooperative systems;

— coordinate the tests carried out on parallel throughout the DRIVE C2X community;

— evaluate cooperative systems;

— promote cooperative driving.

DRIVE C2X will test and evaluate both safety and efficient related services. The DRIVE C2X reference system implements a JAVA/OSGi runtime environment for applications.

#### 5.6.5 Car-to-car communication consortium (C2C-CC)

C2C-CC (CAR 2 CAR Communication Consortium) is a European based membership organization related to C-ITS. C2C-CC has several membership classes: partner, associate membership and development membership. Only vehicle manufacturers can be partners. Currently there are 12 partners of C2C-CC. The mission and the objectives of the CAR 2 CAR Communication Consortium are:

— the development and release of an open European standard for cooperative Intelligent Transport Systems and associated validation process with focus on Inter-Vehicle Communication Systems;

— to be a key contributor to the development of a European standard and associated validation process for Vehicle-2-Roadside Infrastructure Communication being interoperable with the specified inter-vehicle communication standard;

— to provide its specifications and contributions to the standardization organisations including in particular ETSI TC ITS in order to achieve common European standards for ITS;

— to push the harmonization of Car-2-Car Communication Standards worldwide;

— to promote the allocation of a royalty free European wide exclusive frequency band for Car-2-Car applications;

— to develop realistic deployment strategies and business models to speed-up the market penetration;

— to demonstrate the Car-2-Car System as proof of technical and commercial feasibility.

#### 5.6.6 EasyWay project on applications for the major EU road network

EasyWay is an European project for ITS deployment on main European road corridors. The project is driven by national road authorities and operators with associated partners including the automotive industry, telecom operators and public transport stakeholders. EasyWay is partly funded by the European Commission as part of the Trans-European Transport Network (TEN-T) programme which is administered by the Trans-European Transport Network (TEN-T) programme.

EasyWay has established a Cooperative Systems Task Force. This task force has selected seven priority services for first deployment of C-ITS. These are: Hazardous location notification, Traffic jam ahead warning, Road works warning, Decentralised floating car data, Traffic information and recommended itinerary, In-vehicle signage, and Parking management. The task force is cooperating with the DRIVE C2X project and has also stated its intention to support CEN/TC 278 and ETSI TC ITS for the standardization of cooperative systems.

#### 5.6.7 COMeSafety and COMeSafety2 projects on road safety applications

COMeSafety was a support action co-funded by the European Commission under the FP6. COMeSafety2 is a follow-up project under FP7. One of the main objectives of COMeSafety2 is to support the development of a minimum of standards for C-ITS as European Norms, and to support international harmonization of standards. COMeSafety2 also wants to coordinate field operational tests (FOTs) by the exchange of test tools and methods.

#### 5.6.8 Amsterdam Group

The Amsterdam Group is a cooperation platform with the aim to enable deployment of C-ITS. The members are:

— ASECAP – European professional association of operators of toll road infrastructures;

— CEDR – European organization for the national road administrations;

— POLIS – network of European cities and regions working together to develop innovative technologies and policies for local transport;

— CAR-2-CAR Communication Consortium.

The stakeholders within the Amsterdam Group have agreed on a roadmap for deployment of certain “day one applications” which are to be implemented from the year 2015.

# 6 Context of EFC

## 6.1 Definition of EFC

The change from traditional road user charging with manually operated toll booths to electronic free flow tolling systems was the birth of a new term:

— Electronic fee collection (EFC).

In ISO 17573 *Electronic fee collection — Systems architecture for vehicle-related tolling*, the term electronic fee collection is defined as follows:

— Electronic fee collection (EFC) is toll charging supported by electronic equipment on board a vehicle.

NOTE The actual payment (collection of the fee) can take place outside the EFC system.

Including the fact that EFC systems nowadays are free flow systems and do not require a wire based data interface for the tolling process, the definition shall be refined to:

— Electronic fee collection (EFC) is toll charging by electronic means via a wireless interface supported by electronic equipment on board a vehicle.

In the context of EFC according to ISO 17573 toll charging is the electronic collection of tolls for vehicle-related transport services. A transport service is related to the use of, or the presence of a vehicle in a toll domain. The toll domain may encompass a road network, a specific section of road (e.g. a bridge, a tunnel or a ferry connection) or a specific area offering a service (e.g. a parking lot or access to a protected area in a city). It could also be any service related to the use of a vehicle in the transport system, e.g. a petrol station enabling the driver to buy petrol by means of EFC.

Financial authorities may define policies for a toll charging environment and the financial environment it shall operate, e.g. whether the toll is a tax or a fee. They may also define policies for the use of certain types of payment means, e.g. electronic purses, and the split of roles between the toll charging environment and the financial systems.

## 6.2 EFC role model and business architecture

### 6.2.1 Role model

The role model for interoperable EFC systems was developed in the CESARE project and is currently standardized in ISO 17573. According to this role model, the Toll Charger is the provider of the tolled infrastructure or transport service and, hence, the recipient of the road usage charges. The Toll Charger is the actor associated with the Toll Charging role (also called "charging of the toll", see Figure 9).

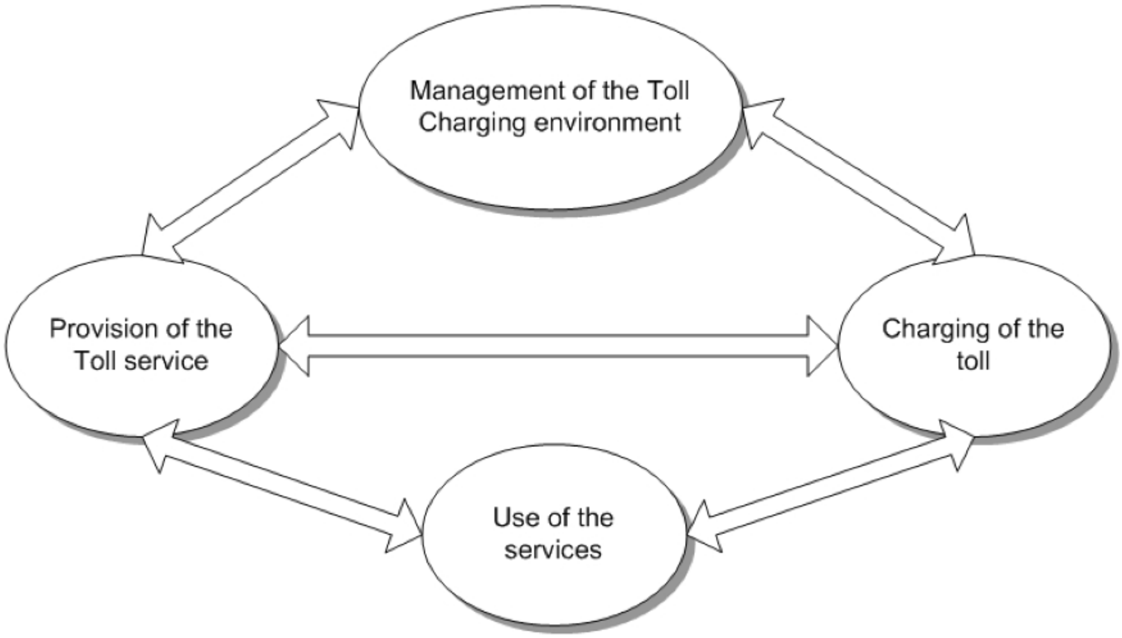



**Figure 9 — The EFC role model [source: ISO 17573:2010]**

Toll Service Providers (i.e. Service Provision role, also called “provision of the toll service”) issue on-board equipment (OBE) to the users (i.e. Service Usage role, also called “use of the service”) of the tolled infrastructure or transport service. Toll Service Providers (TSP) are responsible for operating the OBE that will be used for collecting data enabling the Toll Charger to send a claim to the TSP for the usage of the infrastructure or transport service. In autonomous systems, each TSP delivers toll declarations to several Toll Chargers, as well as each Toll Charger receives toll declarations from more than one Toll Service Provider. In DSRC systems the Toll Charger gets the main toll declarations from its own RSE and only supplementary charging data, if required from the Toll Service Providers. The role “managing of the toll charging environment” in Figure 9 (also called Interoperability Management in the EETS roles model, see Annex D in ISO 17573) comprises all specifications and activities that in common define and maintain a set of rules that govern the overall toll charging environment.

### 6.2.2 Business architecture

The business architecture for EFC systems in this report is defined by four main stakeholder groups based on the role model. This architecture excludes possible value added service roles because this approach is described in CEN/TR 16219, *Electronic Fee Collection — Value added services based on EFC on-board equipment*. The four main stakeholders are:

— Service User;

— Toll Service Provider;

— Toll Charger;

— System Management.

- **Service User (SU):**

The Service User group consists of road users and recipients of transport-related value-added services. This group is represented either by the vehicle operator, the driver or the owner depending upon the nature of the service and the contract terms. In the case of private vehicles the driver and owner will mostly be the same user. The Service User for commercial vehicles will mainly be the fleet manager.

The Service User is responsible for selecting a Toll Service Provider for any road usage within a charged network or networks. The Service User does not need to procure separate tolling services for each individual Toll Charger network. A single tolling offer spanning all relevant charged networks may instead be procured from a Toll Service Provider which integrates all tolling services. This structure is aligned with the EETS service provider model defined in the EETS Directive and allows the Service User to procure all tolling services through a single business relationship. The SP supplies the Service User with an OBE and the Service User is responsible only for ensuring that the OBE is operating correctly. All other operational tolling processes such as fee calculation are managed by the SP.

- **Toll Service Provider (TSP):**

The Toll Service Provider is the provider of all tolling services to the Service User. The Toll Service Provider establishes and maintains direct business relationships with all relevant Toll Chargers on behalf of the Service User and delivers electronic tolling functionality to the user through the provision of an OBE. The relationship between the SP and user is governed by a single contract spanning each of the charged networks required by the Service User.

- **Toll Chargers (TC):**

The Toll Chargers (TC) group includes all owners of road networks, for which a fee is payable by the road user. Toll Chargers may operate regionally, nationally or across international borders, but, unlike a Toll Service Provider, do not offer tolling services for all required networks. The recommended business architecture therefore involves delivery of tolling services via a SP rather than directly to the Service User, as this could lead to a large number of agreements, which could also not all be delivered through a single OBE. A direct relationship is therefore recommended between each Toll Charger and the SP, which can then combine individual fees into a single tolling offer for the Service User. The direct relationship between the TC and Service User is limited to ensuring compliance with all applicable tolling regulations, as outlined in the 'Service User' section above.

- **System Management (SM):**

The System Management includes the government authority of a local or of any state in case of an interoperable EFC system. In case of a local EFC system, this is an optional role. In addition the System Management defines only the legal framework and has no business connections with the other roles.

## 6.3 Technical architecture

### 6.3.1 Overview

The technical architecture of an EFC system is based on two main technical approaches:

— either on an autonomous system approach using multi localization technologies on board (GNSS, CN, DSRC) with an autonomous EFC Front-End;

— or on localization by road side equipment based on DSRC technology.

An EFC system (e.g. an interoperable EFC system like EETS) may also support a combination of both technologies. Figure 10 illustrates the data flows and the main functional components of such a combined system approach.

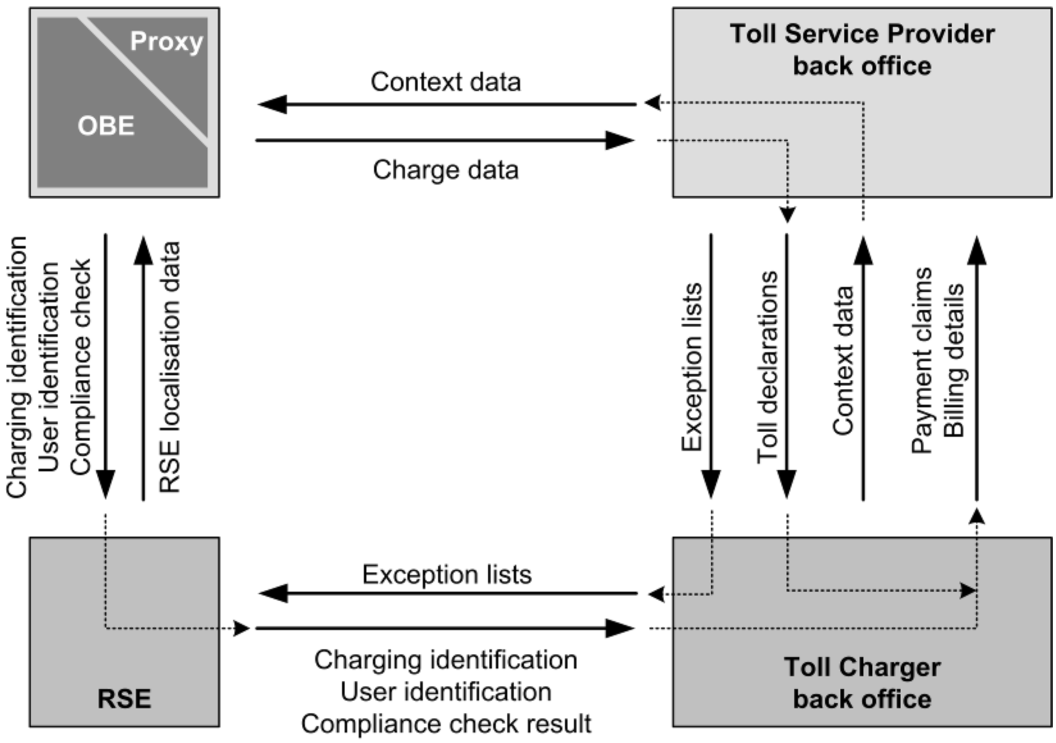



**Figure 10 — Data flow view of the technical architecture**

The description below explains the function of the different OBE types and the functions of the other components in a combined EFC system.

- **Autonomous OBE (EFC Front End):**

The Front End or autonomous OBE for EFC is composed of an OBE and an optional proxy, according to the general EFC Front End architecture defined in CEN ISO/TS 17575 (all parts). The Front End is the equipment through which the charging data are collected. Depending on technical concept, the charging data are completely generated on the OBE or only raw data are collected by the OBE and the charging data are generated on the proxy (see also 6.3.3). The autonomous OBE is for enforcement reasons and localization support equipped with a DSRC interface.

The Front End generates:

— information to be transmitted to the user, via the OBE's HMI;

— charging data to be further processed in the Toll Service Provider back-office.

The Front End interface to the TSP back-office provides for the following exchange of data:

— charging data which are generated by the Front End;

— EFC applications update as well as toll domain context data updates received from the Toll Charger back-office for deployment at the Front End.

- **DSRC based OBE:**

The OBE for a road side based EFC system has as its main function only a DSRC interface for tolling and enforcement purposes. The main functionality in this EFC system approach, collecting charging data, is located at the RSE.

- **Road side equipment (RSE):**

The RSE has three different tasks:

— collect road usage data (charging identification, specified e.g. in EN 15509);

— perform vehicle and OBE (i.e. user) compliance check (CCC) (specified in CEN ISO/TS 12813);

— support vehicle localization by transmitting RSE localization data (LAC) (specified in CEN ISO/TS 13141)

Compliance check is done by the use of data read out through the DSRC interface of the OBE, in combination with vehicle classification and automatic number plate recognition (ANPR) technologies.

- **Toll Charger back office:**

The Toll Charger back office calculates the payment claims either from the toll declarations received from the service provider back office or from the charging data collected by its own RSE. The TC back office manages and distributes also the EFC context data to the Toll Service Providers.

It also receives the exception lists of the TSP and possibly manages exception lists of the Toll Charger. Exception list will be distributed to the RSE of the TC for immediate identification and enforcement of vehicles and users on the exception lists.

- **Toll Service Provider back office:**

The Toll Service Provider back office is responsible for managing and deploying the OBE parameter including the context data to the Front End. In an autonomous OBE system it collects the toll declaration of the Front End and forwards this data to the corresponding Toll Charger back office. The payment claims and billing details received from the Toll Chargers are used to calculate the invoices to the users.

The Toll Service Provider Back-office implements the Customer Relationship Management, billing and invoicing processes of Service Users for EFC. Payment (collection of the fee) is handled between Toll Service Provider and Service User. The Toll Service Provider guarantees the payment to the Toll Charger. The back office routes charge data generated by the Front End summarized as toll declarations to the Toll Charger back-office.

The TSP back office also manages exception lists of OBE and its users which are no longer valid for collecting charging data (e.g. the user black list). This list is distributed to the Toll Chargers.

- **Service point equipment:**

Figure 11 shows a possible additional component of the TSP, the customer and OBE service point. If required, this service point equipment uses an interface to load personalisation data, OBE parameters and software to the OBE. This service point equipment will receive and store the required data from and in the service provider back office.

### 6.3.2 Communication architecture

Figure 11 illustrates as an example the component and interface view of an EFC system supporting both, the autonomous and road side based approach. The numbered EFC related interfaces (1 to 3) are more or less completely defined by standards:

1) The 5,8 GHz DSRC communication layers (layer 1 by EN 12253, layer 2 by EN 12795, application layer by EN 12834) the application interface (EN ISO 14906), the charging communication application (EN 15509), compliance checking communication (CEN ISO/TS 12813) and the localization augmentation communication (CEN ISO/TS 13141). The 5,8 GHz DSRC communication applicable in Italy is defined by the UNI (Telepass) standard according to ETSI ES 200674-1.

2) Service Provider to Toll Charger back office interface defined by EN ISO 12855.

3) Autonomous OBE (Front End) to TSP back office interface defined by CEN/ISO/TS 17575 (all parts).

The positioning interface uses mostly the GPS signal. GLONASS, EGNOS and in future Galileo are also possible positioning systems. The other communication interfaces are defined internal by the Toll Charger or the Toll Service Provider as required by the individual system solution.

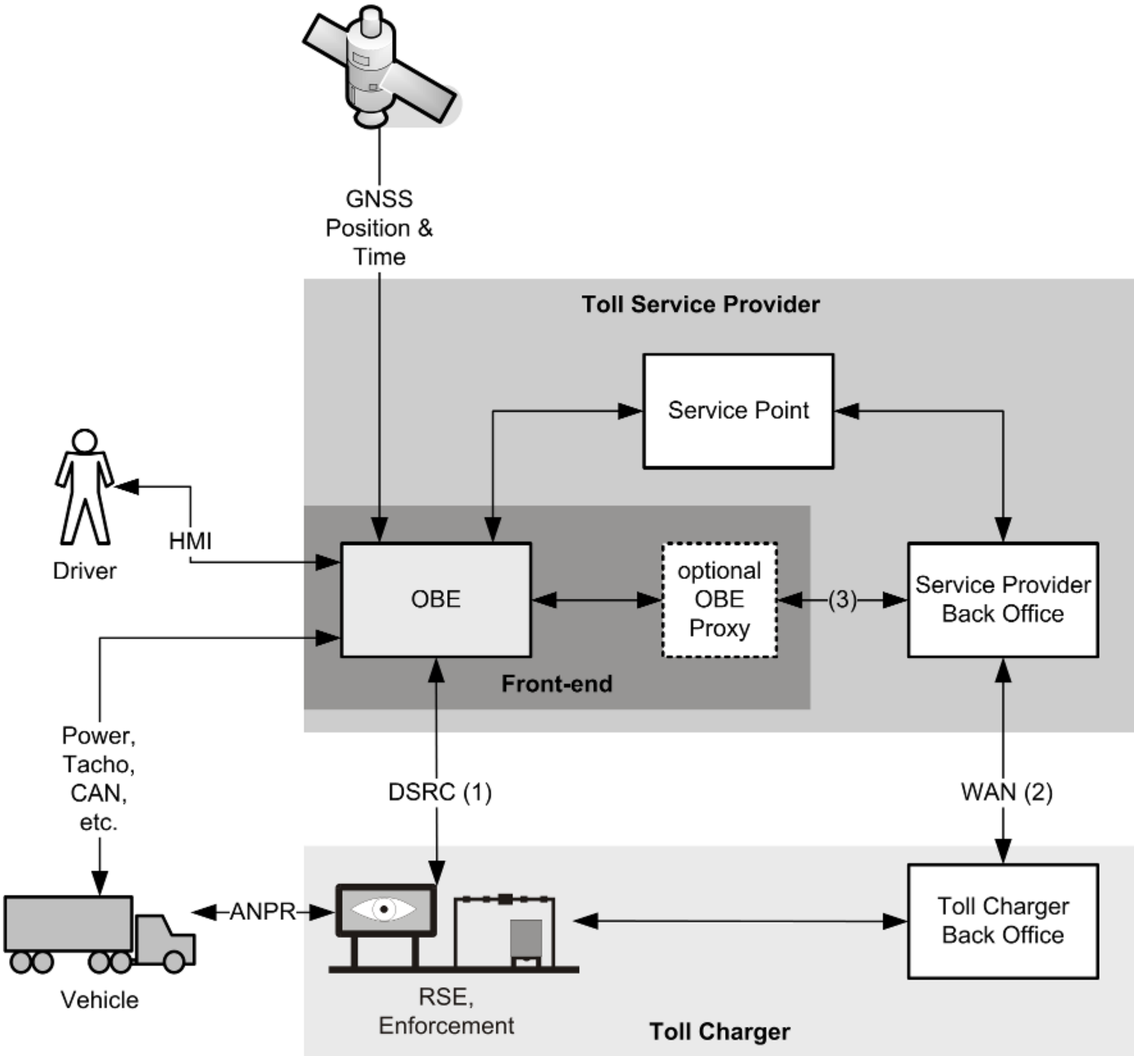



**Figure 11 — Component and interface view of the technical architecture**

NOTE There are further interfaces to the external world which are not presented in the figure: Examples of such interfaces are from/to fleet card providers, financial institutes, payment service providers, public authorities, call centres, mass printing providers.

### 6.3.3 Autonomous OBE / Front End implementation

The OBE (i.e. the Front End) for autonomous systems can be implemented in a thick client or thin client systems architecture, with potentially any shades of grey between the thin and thick extremes. Figure 12 illustrates the different functional steps of the charging process and where these steps are executed according to the selected system architecture approach.

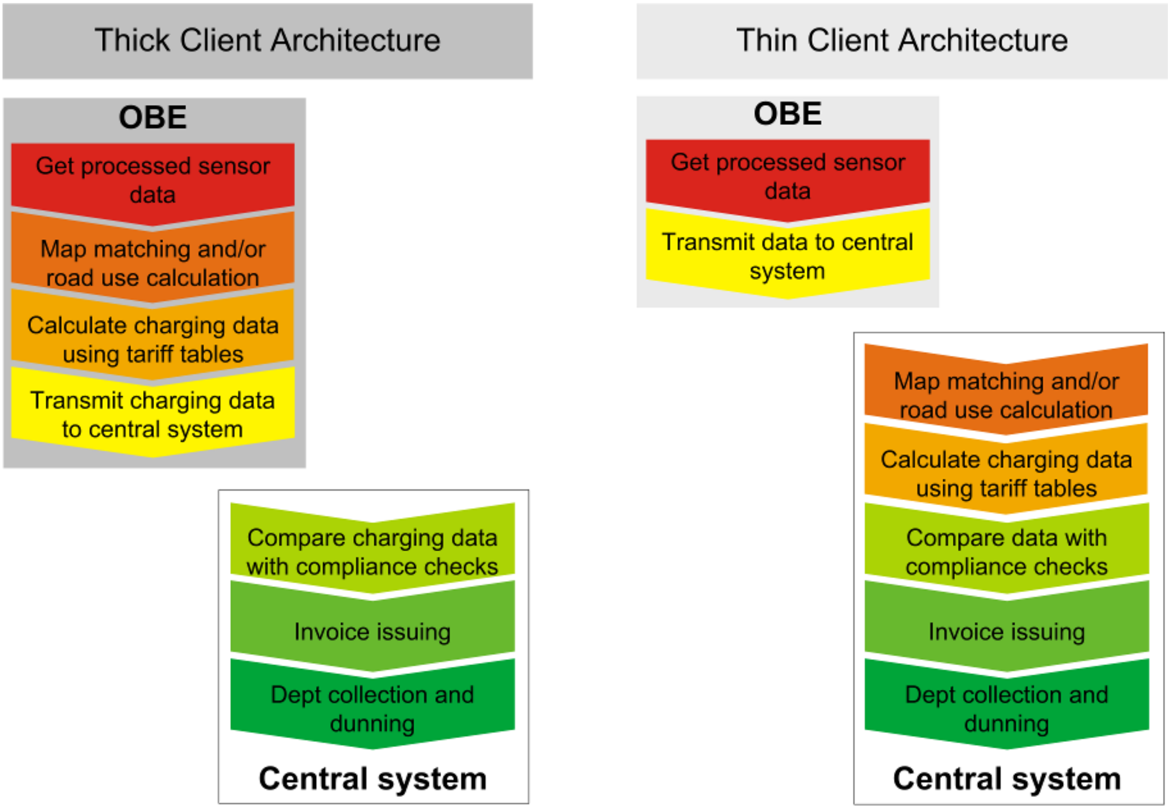



**Figure 12 — Examples of data processing steps in thin and thick client approaches**

The “thick” OBE (also called Smart or Thick Client) in the thick client approach performs most parts of the data processing steps by means of OBE internal functions. This includes the map-matching algorithms to determine the used road segments. Then the tariff tables are applied to calculate the charge. A first operational EFC system in Europe using thick OBE was realized in Germany (refer also to 6.7.2).

The “thin” OBE (also called Thin Client) in a thin client architecture will perform only limited data processing steps within the OBE. Most data processing is performed in central computing facilities. The French system (l’éco taxe poids lourds, TPL) is using for some OBE types such an approach.

### 6.3.4 EFC security

The ETSI ITS security standards may be applicable and useful for EFC. In addition CEN/TC 278/WG 1 has developed special, EFC related security standards:

— CEN/TS 16439, *Electronic fee collection — Security framework*;

— EN ISO/TS 17574, *Electronic fee collection — Guidelines for security protection profiles* (ISO/TS 17574*)*;

— two parts of the secure monitoring standard under development in CEN/TC 278/WG 1 (*Part 1: Compliance checking*, and *Part 2: Trusted recorder*).

The security framework defines EFC security requirements and security specification for a whole EFC system. The EFC security framework specifies the missing security measures in detail for the standards mentioned in 6.3.2. The second standard is a guideline for the definition of protection profiles according to the common criteria defined in ISO/IEC 15408 (all parts). The secure monitoring standards are dealing with the compliant behaviour of the road user. They will help avoiding and detecting of possible fraud caused by illegal manipulations of the OBE by the user.

More detailed security considerations are provided in Annex A of this Technical Report.

## 6.4 Additional major aspects

### 6.4.1 Interoperability

EFC interoperability is mostly driven by political ambitions to improve mobility and the efficiency of transport systems. Examples of interoperable EFC projects are EasyGo in the Scandinavian countries and the future EETS in the European Union.

Interoperability is defined as the ability of systems to provide services to and accept services from other systems and to use these services to enable the systems to operate effectively together (source CARDME-4). For EFC systems three different parts or levels of interoperability have to be considered: Technical, procedural and contractual interoperability.

— Technical interoperability is the capability of different sets of equipment to work together through interconnection, coordinated execution or sharing of resources.

— Procedural interoperability is given by the existence of common data element definitions, the same working procedures and data delivery and common format of presentation in different sets of equipment required to communicate.

— Contractual interoperability is the intention of operators to co-operate recorded in a contractual agreement.

If two EFC systems are fully interoperable, then all three interoperability levels, the technical, the procedural and the contractual interoperability have been solved.

An example of partly interoperability is to use only the technical and the procedural interoperability level. In such case the user has still a contract with each operator (because of the missing contractual operator agreement). This approach was used for the interoperable use of the Swiss LSVA OBE in the Austrian EFC system.

### 6.4.2 Value added services based on EFC OBE

Value added services (VAS) on EFC OBE has been analysed in detail in [CEN/TR 16219]. As VAS on EFC OBE is something like the opposite approach investigated in this Technical Report, a short introduction can be found below.

- **Definition of VAS:**

In the context of EFC, a value added service (VAS) in this strict sense is a telematics service offered to the Service User by means of the EFC OBE. This service might directly be consumed by the driver in the vehicle, or might, particularly in the case of heavy vehicles, be targeted at the freight operator and be consumed in a back office. Such services can be fleet management services like track-and-trace, payment services such as paying petrol automatically at the pump, or regulatory applications such as Electronic Vehicle Identification (EVI) or Access Control. Such additional services and applications create additional value to the user either by the value the new service creates to him, or in the case of regulatory services, by combining several functionalities in a single device, thus removing the need to install and maintain several pieces of equipment simultaneously.

In a wider sense, the operator of the EFC service can draw additional benefit from the data collected by the EFC system. Data from EFC OBE give a good account of the traffic situation on the charged network, and may be utilized either for statistical purposes, for traffic planning or even in real time for traffic information purposes.

The Technical Report CEN/TR 16219 on VAS based on an EFC OBE has identified potential applications according to the definition above and grouped them into application classes for the analysis as potential VAS on EFC OBE. The application classes are:

— fleet management;

— entertainment;

— payment;

— cooperative road safety;

— driver assistance;

— communications;

— navigation and traffic information;

— traffic data collection;

— vehicle usage recording;

— regulatory applications.

The major findings in CEN/TR 16219 described below are considered in this Technical Report because they are also important despite the fact that EFC on ITS Station is a different, possibly opposite approach.

- **Key design drivers:**

There are three main design drivers for delivering VAS from the EFC OBE platform:

— The first driver is whether or not there are synergies, i.e. benefits from a joint delivery both in technical and in business terms.

— The second driver is that the tolling functionality shall not be compromised in any way by a VAS application.

— Finally, the third driver is the platform architecture including the related operational and cost aspects of delivering tolling and VAS through the same OBE.

- **Uncompromised EFC functionality:**

The requirements of the EFC application are described in Clause 7 in this CEN/TR and have to be fulfilled independently of any VAS application. This includes uninterrupted detection of all tolling events including regular transmission of charge data, data exchanges at scheduled moments as well as communication with road side equipment and mobile enforcement units. For this reason an appropriate computing architecture has to be in place at the tolling platform to allow operation of the EFC and VAS application with defined availability, performance and security.

- **Certification issues:**

EFC, especially the EETS, require that OBE including the tolling application is certified. While the exact procedures and requirements are far from unambiguously specified and implemented at the moment, it can be expected that an OBE would lose its certification if it were to allow any arbitrary VAS to be executed. In principle, an OBE can only be certified together with the EFC application and all eventual VAS applications. Such a process is not foreseen in the EETS. For reasons of governance, certification agencies will most likely only have the necessary processes and rules in place to certify for compliance with the EETS and will not be able to certify VAS that run concurrently on platforms.

- **Supporting VAS on an EFC platform:**

Opportunities for supporting VAS exist where resources and vehicle data existing within the EFC Platform can be shared with other selected VAS applications without compromising the performance of the tolling application or resulting in other functionality conflicts.

The synergies can reduce the overall cost of providing both tolling and VAS applications when compared with the use of completely separate platforms for each service. According to the actual VAS application to be supported, a certain approach can be implemented. A viable solution would be an EFC platform for VAS which would be able to support the following three approaches: supporting some selected integrated VAS applications, like payment over DSRC, partly integrated applications like fleet management, and additional loosely coupled applications on an additional device.

### 6.4.3 EFC outside Europe

The scope of this Technical Report is limited to EFC in Europe. However, to give a broader picture the paragraphs below present a brief overview on the situation of EFC in other regions.

EFC in the United States is a wide spread service at is used by millions of road users every day. Compared to Europe significantly more EFC OBE are deployed and in commercial use. Almost all EFC systems in US apply a single lane topology. One can also find EFC based services for HOT and HOV lane applications which are not used in Europe at all.

With respect to the applied EFC technology almost all EFC systems in US base on a DSRC principle. However, compared to Europe a different frequency band is in use. EFC in the US applies 915 MHz technology. Such frequency band allows – in comparison with the CEN TC 278 DSRC technology – the optional use of passive OBE/tags (so-called sticker tags). On the other hand 915 MHz DSRC technology has limitations in free-flow multi-lane environment. Furthermore, passive OBE and the applied data protocols lack sophisticated security mechanisms. In contrast to Europe where one single interoperable DSRC specification and technology in use (except for Italy), the US market shows a regional fragmentation into areas with different specifications and protocol standards. The various specifications are not interoperable amongst each other. If interoperability is achieved, then so-called multi-protocol readers are in place. Such EFC RSE is capable to exchange data with OBE following different standards.

CN/GNSS based EFC in North America is known from trials and currently not in commercial use in larger scale.

Australia has adopted the European CEN TC 278 set of EFC standards a long time ago. Multi-lane and single lane EFC systems are in a very successful operation in particular in the metropolitan regions in Australia for many years. As a result of the use of an interoperable technology a very competitive market with respect to EFC RSE and OBE equipment has developed. There are plans for a potential introduction of a CN/GNSS based EFC system for trucks.

EFC is widely deployed in several countries in *Asia*. Large scale EFC systems can be found in Japan, Malaysia, China, Taiwan, Singapore and other countries. Each of these countries applies a different EFC technology. There are e.g. active 5,8 GHz DSRC, infrared based DSRC, and other local, national and proprietary standards.

## 6.5 Legal aspects and background

### 6.5.1 Toll domain specific

Depending on the target of an EFC system, e.g. infrastructure financing, improving of road traffic efficiency by reduction or redirection of traffic flows, each toll domain may have its independent and specific laws and regulations.

In the EU the freedom of such legislation for heavy vehicles with a maximum permissible weight with 3,5 t and above is limited by the Directive 2011/76/EU amending Directive 1999/62/EC on the charging of heavy goods vehicles for the use of certain infrastructures.

### 6.5.2 European Electronic Toll Service (EETS)

- **EU Directive 2004/52/EC:**

Interoperability of road charging solutions is a long-term objective of the EC. In April 2004, Directive 2004/52/EC of the European Parliament and Council on the interoperability of electronic road toll systems in the Community was adopted. The Directive places constraints on the technologies that may be used in future new road charging systems:

— satellite positioning;

— mobile communications using the GSM-GPRS standard;

— 5,8 GHz microwave technology.

The new road charging service that should be interoperable throughout Europe on the basis of one or more of the mentioned technologies is called the European Electronic Tolling Service (EETS). In a summary this directive describes the following:

— operators and Member States are obliged to accept interoperable OBE that are compliant with the EETS;

— operators are obliged to provide this service and OBE to end users;

— the end user can make use of this service and related OBE on a voluntary basis.

- **EU Commission Decision 2009/750/EC:**

The EC has provided in October 2009 a more detailed definition of the EETS service in the Commission Decision 2009/750/EC. The Decision sets out the essential technical specifications and requirements needed to launch EETS. In addition the Decision lays down the rights and obligations of Toll Chargers, service providers, and users.

The Decision stipulates that each EU Member State with an electronic toll collection system in operation on its territory shall keep a national electronic register with information on the domain of EETS relevant toll roads, the Toll Chargers concerned and the EETS providers, if any, having contracts with these Toll Chargers, respectively EETS providers that had been granted registration by the Member State.

- **Guide for the application of the directive on the interoperability of electronic road toll systems:**

In 2011 the European Union published a guide for the application of the Directive. The objective of this guide is to help clarify certain concepts and procedures referred to in Directive 2004/52/EC on the interoperability of electronic road toll systems and the related Commission Decision 2009/750/EC on the definition of the EETS. In particular, the guide aims to explain how EETS interoperability constituents might be assessed with a view to meeting the essential requirements of Decision 2009/750/EC.

#### 6.5.3 User privacy and data protection

User privacy and data protection may become a crucial issue when setting up an EFC system. EFC systems are intrinsically linked with the movement and exchange of personal data. In addition EFC is a payment application, often with deep legal implications in case of non-payment or fraud. Integrity of the collected road usage data, including vehicle identity, payment account and user declarations, is of high importance.

The relevant EU legislation concerning user privacy and data protection in EFC systems is Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector) for the processing of personal data.

### 6.6 Overview of standardization activities

#### 6.6.1 CEN/TC 278/WG 1 on Electronic fee collection and access control applications

CEN/TC 278/WG 1, *Electronic fee collection and access control*, is responsible for European standardizing of the EFC application, while other international standardization groups provide standards on supporting technologies (such as GNSS) and communication protocols. Most EFC standards are developed as joint work items with ISO/TC 204, under CEN lead (the WG is also a working group within ISO; ISO/TC 204/WG 5). In addition ETSI provides certain technical standards on the use of the frequency spectrum and testing that are vital for the EFC area.

The current standardization work includes defining application interfaces between equipment, information flows between EFC operators, architecture, security, conformance evaluation and test standards, personalisation of OBE, performance indicators and enforcement/monitoring support.

EFC standardization in CEN/TC 278/WG 1 is divided roughly into the following key areas:

— DSRC-based EFC standards (including test standards);

— autonomous (GNSS/CN-based) EFC-standards (Including test standards);

— technology-independent standards (architecture, security, information flows, smart cards, etc).

The European Electronic Toll Service (EETS) is being set up for interoperable EFC systems in Europe called for by Directive 2004/52/EC on the interoperability of electronic road toll systems in the Community. This Directive lays down the conditions necessary to ensure the interoperability of electronic road toll systems in the European Union. A mandate, M/338, on how standardization could support these efforts has been initiated; under this mandate. CEN and ETSI are working closely together with the EC on standards that will support the EETS. CEN/TC 278/WG 1 provides the standards that form the main building blocks for defining this interoperable service.

Much of the standardization work undertaken builds on the work and achievements from European EFC projects, such as CARDME, CESARE-4, PISTA, MEDIA and RCI.

#### 6.6.2 ISO/TC 204/WG 5 on electronic fee collection and access control applications

ISO/TC 204/WG 5 is a joint working group with CEN/TC 278/WG 1.

#### 6.6.3 ETSI Technical Committee for ITS (ETSI TC ITS)

ETSI Technical Committee for ITS does not develop specific EFC standards. But the ETSI TC ITS/WG 4 has developed a test standard for DSRC (ETSI/TS 102 486). For the major part of the activities carried out in ETSI TC ITS, see 5.5.6.

## 6.7 Examples of commercial projects

### 6.7.1 Small EFC system: Herrentunnel Lübeck (Germany)

The Herrentunnel in Lübeck (Germany) is one of the two projects that have been initiated and commenced by the German Ministry of Transport in order to create new road infrastructure objects (tunnels in this case) under the involvement of private concessionaires. The project follows a DBOF (design, built, operate and finance) principle.

The Herrentunnel project was awarded in 1999 and set into full operation in 2005. The consortium of the concessionaire comprises HOCHTIEF Solutions AG und BILFINGER BERGER Project Investments Corporate Services GmbH. The overall investment amount is in the range of about 175 Mio EUR.

The tunnel replaces a bridge that connected two districts of the city of Lübeck. The bridge was not capable to cope with the increasing traffic demand. During peak hours massive congestion appeared. In contrast the tunnel provides a road with two lanes at each of the two separated carriageways. The length of the concession road is about 2 km.

Road users pay the respective toll fee at a toll plaza. The level of the toll fee is determined by the vehicle category. All vehicles classes are subject to the toll. The following types of payments are accepted by the operator of the plaza:

— cash;

— contactless chip card;

— EFC by means of a DSRC On-board Equipment (OBE);

— fleet cards.

DSRC OBE can be used at all lanes. However, in order to make the use of ETC attractive to the road users a dedicated ETC lane per driving direction is also available at the toll plaza. These dedicated ETC lanes enable a sort of “slow-and-go” method that prevents ETC users from queuing at the barriers in the other lanes. In addition the toll rates for users of ETC OBE are significantly lower compared to the rates for cash and card payments.

The ETC technology installed at the lanes of the toll plaza is compliant to the 5,8 GHz CEN TC 278 standards suite. OBEs are simple to use DSRC based on-board device which are fitted to the windscreen and are powered by an internal battery that lasts about 7 years.

Despite technically possible the concessionaire does not support interoperability of the ETC solution with other ETC systems in Germany or Europe. The reason is the rather local and regional significance and focus of this piece of road infrastructure. Therefore Herrentunnel project is not considered as an EETS toll domain.

### 6.7.2 Nationwide EFC system: Germany

The Federal Government, specifically the German Ministry of Transport, Building and Housing introduced on January 1st 2005 a new EFC system for charging of all HGVs using the German Motorway network on the basis of the distance travelled. The project is organized as a Private Public Partnership (PPP). The private company Toll Collect GmbH is responsible for collecting the toll on behalf of the Ministry. For this service it gets a service fee, so called operation compensation.

All vehicles with a permissible weight of 12 tonnes and above which are exclusively intended for use in transporting freight pay a toll based on the distance travelled on the motorway network in Germany. The new tolling scheme replaces the paper-based Eurovignette scheme. The charged road network was extended in 2012 by additional 1 000 km of federal roads.

There is a dual toll collection system with a main scheme solution using an OBE and an occasional user scheme with manual journey pre-booking. The charge-payers have a free choice between the main scheme and occasional user scheme. The use of OBU is not mandatory.

In the main scheme the users obtain suiTable OBE for the vehicle. For the installation of the OBE an extensive network of 1850 service outlets exists.

The OBE will automatically log and register journeys on the charged network. The equipment incorporates a digital map of the charged roads as well as satellite based location (GPS) facilities. There are also gyroscopes to detect vehicle movements and turns. This equipment monitors the position of the vehicle. It recognizes when passing a virtual toll gantry. Once on the charged network, the unit identifies each road segment subject to toll and determines the length by reference to the in-vehicle map.

The OBE calculates the toll based on preset vehicle parameters (number of axles, weight, and emission class), rate information and the number of kilometres travelled. The OBE uses a GSM cell network communication to send charge information to the back office.

#### 6.7.3 Interoperable EFC system: EasyGo

EasyGo is a partnership between toll plaza operators, toll roads, bridge companies and ferry operators. The purpose is to enable road users to drive through all the toll facilities they might encounter on your way through Northern Europe – quickly and easily. The intention is for road users to have one payment system only - whether it is a BroBizz, an AutoPASS or an AutoBizz DSRC OBE - for payment throughout Europe. EasyGo currently covers Northern Europe (i.e. Denmark, Sweden and Norway), from Puttgarden in the south to Northern Norway. Additional toll stations are joining the partnership all the time.

Any customer using an OBE issued by an EasyGo issuer can use it for toll charging at any operator offering the EasyGo service. The technology used in the different OBEs for the EasyGo system is 5,8 GHz DSRC with different EFC transaction protocols, i.e. AutoPASS and PISTA I.

The EasyGo system is applicable for heavy and light vehicles. Depending on the toll road, bridge or ferry different occasional user solutions are available, e.g. cash payment in a separate lane or registration of the licence plate with payment by credit card or invoice after vehicle detection by ANPR.

## 7 Outline of EFC requirements to an ITS Station

### 7.1 High level EFC requirements

The following high level requirements for EFC applications have been identified in CEN/TR 16219:

— The EFC System shall ensure the correct toll income to the Toll Charger.

— The EFC System shall ensure a fair and equal treatment of users.

— The EFC System shall be simple and transparent for its users.

— The EFC System shall ensure reasonable operational costs to the Service Provider.

In order to design systems that fulfil such high level requirements more detailed and underlying requirements of different type and nature have to be specified and fulfilled.

Such underlying requirements relate to:

— various areas (like functional, technical, performance, operational, security, life-cycle);

— various ITS Station types (in-vehicle ITS station, porTable ITS station, central ITS station and road-side ITS station); and

— various business roles (e.g. EFC Toll Charger, EFC service provider, C-ITS System Manager, C-ITS System Operator, Policy Framework).

The following subclauses outline the major requirements which need to be fulfilled to enable EFC services and support meeting the abovementioned high level requirements.

NOTE 1 It is essential that the high level requirements and the underlying (more functional and technical) requirements listed in this and the following subclauses are not understood as “formal” low level technical requirements which can be used as is as for the purpose of design, implementation and testing. However, they provide the base for such low level technical requirements. Low level technical requirements are subject of Technical Standards or other specifications. They are outside the scope of this Technical Report. See also the definition of the scope and non-scope of this Technical Report in Clause 1.

For the propose of the next subclauses it is assumed that the EFC application(s) which provide the EFC charging services to the road user respectively the EFC enforcement service to the EFC Toll Charger are enabled and operated in the C-ITS environment. This means the EFC services are considered being registered services in the ITS and the required EFC application(s) are available on the ITS Station(s).

The requirements are split into two groups:

— requirements to the EFC service / application(s) on the ITS Station (see 7.2);

— requirements to the ITS Station itself or connected sensors or supporting functions (like facilities) (see 7.3).

This structure and how the different requirement levels relate to each other are outlined in Figure 13.

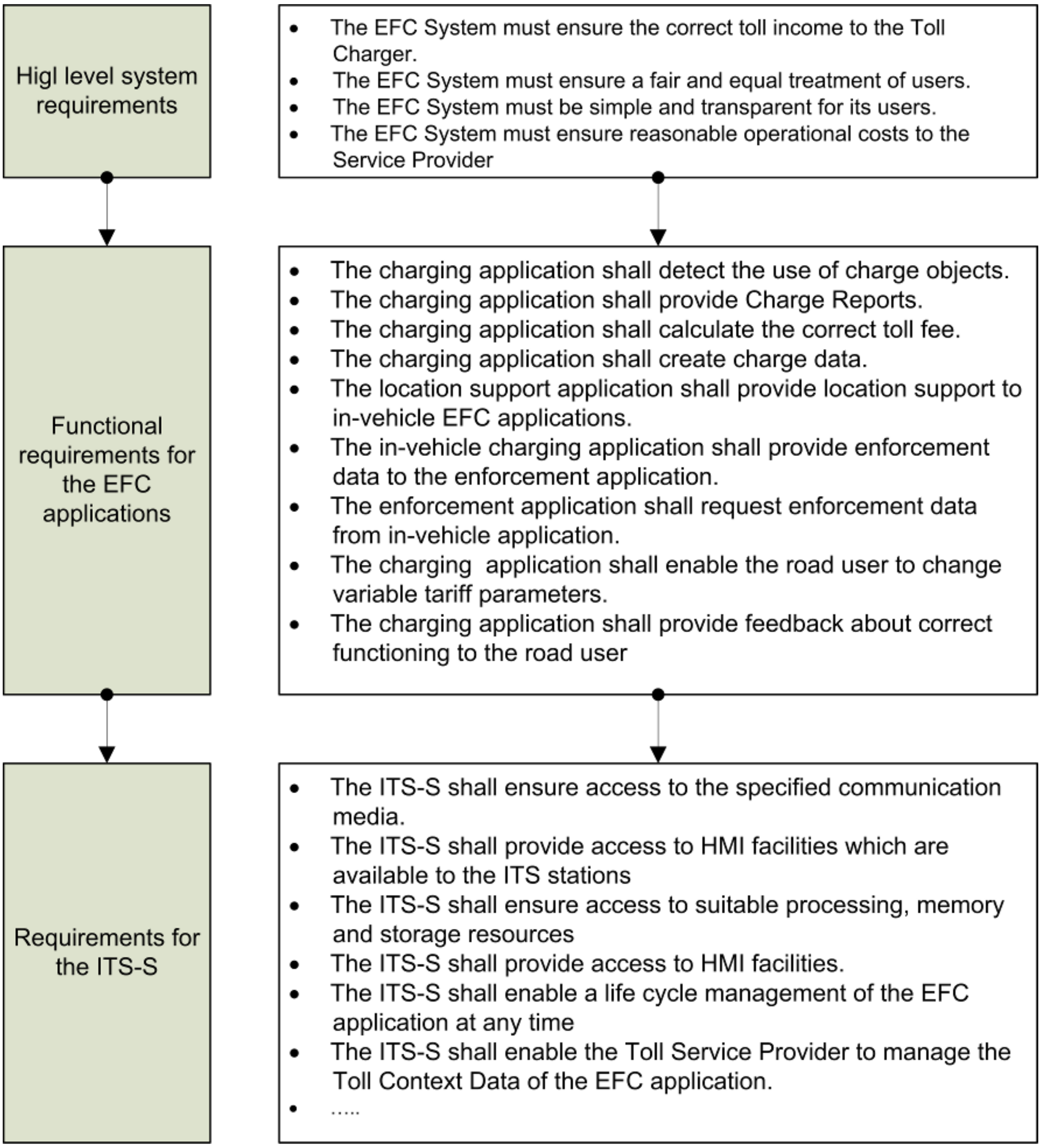



**Figure 13 — General requirements structure (Example)**

NOTE 2 Some of the requirements Figure 13 are optional. Not all requirements are provided in this figure.

NOTE 3 No distinction has been made with respect to requirements applying to the ITS-S and ITS-SU.

For the avoidance of doubts: Finally the EFC applications have to fulfil the requirements. However, as the EFC application makes use of technical resources, functions and processes which the ITS-SU – as an application independent platform - provides also the ITS-SU has to comply with particular underlying requirements.

## 7.2 Requirements for the EFC application(s)

### 7.2.1 Detection of Charge Objects (autonomous toll domains)

Requirement: The EFC application shall detect the use of charge objects.

Remarks / Conditions:

a) The type of a charge object (road section, area, and cordon) depends on the individual Toll Context.

b) This requirement is valid in autonomous toll domains only.

c) Details of the charge objects and their description are provided in the toll context data (CEN ISO/TS 17575-3:2011, 8.3.4 and Annex A and CEN ISO/TS 17575-4:2011, Clauses 6 and 7 and Annex A).

d) This requirement may imply the need to use location support (provided by a location augmentation application):

   1) location augmentation communication shall be compliant to CEN ISO/TS 13141;

   2) the availability of location augmentation is toll domain specific.

Applicability:

— in-vehicle ITS Station (autonomous toll domains);

— central ITS Station (optional proxy in autonomous toll domains).

Involved EFC roles:

— Toll Service Provider

#### 7.2.2 Provision of charge reports (autonomous toll domains)

Requirement: The EFC application shall provide charge reports.

Remarks / Conditions:

a) The charge report shall comply with the specifications outlined in CEN ISO/TS 17575-1:2010, Clauses 5 and 6 and Annex A.

b) The charge report Configuration as specified in CEN ISO/TS 17575-3:2011, 8.3.5 and Annex A provides Toll Context depended details on:

   1) required content of the charge report;

   2) events that trigger the provision of a charge report.

Applicability:

— in-vehicle ITS Station (autonomous toll domains);

— central ITS Station (optional proxy in autonomous toll domains).

Involved EFC roles:

— Toll Service Provider

### 7.2.3 Fee calculation (autonomous toll domains)

Requirement: The EFC application shall calculate the correct toll fee[3].

Remarks / Conditions:

a) The fee calculation shall follow the rules applicable in the individual Toll Context.

b) The fee shall be calculated using the tariff determining parameters as specified in CEN ISO/TS 17575-3:2011, 8.3.3.3 which are:

   1) vehicle classes;

   2) user classes;

   3) location classes;

   4) time classes.

c) This requirement is optional as – depended on the rules applicable in the individual toll domain – the fee may be calculated by the Toll Charger (and not by the Toll Service Provider).

Applicability:

— in-vehicle ITS Station (autonomous toll domains);

— central ITS Station (optional proxy in autonomous toll domains).

Involved EFC roles:

— Toll Service Provider;

### 7.2.4 Generation of charge data (DSRC based toll domains)

Requirement: The EFC application shall create charge data in DSRC toll domains.

Remarks / Conditions:

a) The EFC application shall use a DSRC communication application based on EN ISO 14906 (e.g. EN 15909 in an interoperable EFC domain).

b) This requirement is valid in DSRC based toll domains only.

Applicability:

— road side ITS Station;

— in-vehicle ITS Station (support of DSRC communication with delivery of required EFC application data).

Involved EFC roles:

— Toll Service Provider;

— Toll Charger.

3) The "fee" may also be a tax, duty or other type of levy.

#### 7.2.5 Location support (autonomous toll domains)

Requirement: The EFC location support application shall provide location support to in-vehicle EFC applications.

Remarks / Conditions:

a) The location augmentation communication shall be compliant to CEN ISO/TS 13141.

b) The need to provide such location support may depend on:

   1) the particular need (e.g. topology) of the toll domain; and

   2) the type and capability of the location functions of the in-vehicle EFC application.

c) The in-vehicle ITS Station may use location support if available.

Applicability:

— road side ITS Station.

Involved EFC roles:

— Toll Charger.

#### 7.2.6 Support of enforcement application

Requirement: The EFC application shall provide data for use in an enforcement application.

Remarks / Conditions:

a) The enforcement application shall support compliance check communication.

b) The compliance check communication in autonomous systems shall be compliant to CEN ISO/TS 12813.

c) The compliance check communication in DSRC based system shall be compliant to EN ISO 14906 and EN 15509 in EETS compliant toll domains.

d) The EFC application shall provide all application data required by the compliance check communication as specified by the Toll Charger of the individual Toll Context.

Applicability:

— in-vehicle ITS Station.

Involved EFC roles:

— Toll Service Provider.

#### 7.2.7 Operation of an enforcement application

Requirement: The enforcement application shall request data from passing in-vehicle EFC applications and enable the detection of road users not behaving according to the rules of the Toll Context.

Remarks / Conditions:

a) The enforcement application shall use compliance check communication.

b) Compliance check communication in autonomous toll domains shall be compliant to CEN ISO/TS 12813.

c) Compliance check communication in DSRC based toll domains shall be compliant to EN ISO 14906 respectively EN 15509 in EETS compliant toll domains.

Applicability:

— road side ITS Station.

Involved EFC roles:

— Toll Charger.

### 7.2.8 Changing variable tariff parameters

Requirement: The EFC application shall enable the road user to change variable tariff parameters.

Remarks / Conditions:

a) The particular variable tariff determinants depend on the rules applicable in the individual Toll Context. These are e.g.:

   1) vehicle class (e.g. number of axles, maximum permissible weight, actual weight, presence of trailer);

   2) user class (e.g. number of passengers).

b) Variable tariff determinants may be changed;

   1) manually by the road user (e.g. via an HMI); or

   2) automatically depending on sensor input (e.g. presence of a trailer).

c) The EFC application shall provide a means for the road user to check the actual parameter setting.

Applicability:

— in-vehicle ITS Station.

Involved EFC roles:

— Toll Service Provider.

### 7.2.9 Feedback to the road user

Requirement: The EFC application shall provide feedback about its correct functioning to the road user.

Remarks / Conditions:

a) Such feedback shall be provided via a suiTable HMI.

b) The feedback shall indicate to the road user if the current operational status of the EFC application allows the use of the toll liable road network in the respective toll domain.

Applicability:

— in-vehicle ITS Station.

Involved EFC roles:

— Toll Service Provider.

## 7.3 Resulting requirements for the ITS Station

### 7.3.1 Technical requirements

#### 7.3.1.1 Access to and compliance with communication media

Requirement: The ITS Station shall ensure access to the specified communication media.

Remarks / Conditions:

a) The availability of the communication media itself are outside the scope and responsibility of the ITS–S. However, the ITS-S shall provide the respective access mechanisms.

b) The communication medium shall comply with the requirements defined by the Toll Charger and comply with the rules set by this Toll Charger for the defined toll domain.

c) This requirement implies the conformance to the related international standards for the communication channel and the applicable protocol stack.

d) Based on the Interoperability Directive 2004/52/EC possible communication media are:

   1) satellite positioning;

   2) mobile communications using the GSM-GPRS standard (reference GSM TS 03.60/23.060);

   3) 5,8 GHz microwave technology.

Applicability:

— in-vehicle ITS Station;

— road-side ITS Station;

— central ITS Station.

Involved roles:

— ITS Station Service Provider (TC and TSP may be regarded as ITS Station Service Provider of their own EFC Back Office System).

#### 7.3.1.2 Support of EFC application data

Requirement: The ITS Station shall ensure storage, updating, managing of application data required by the EFC application.

Remarks / Conditions:

a) The detailed data specifications depend on the needs of the Toll Charger and Toll Service Provider.

b) This requirement implies the conformance to the related international standards for EFC application data, i.e. EN ISO 14906, EN 15509, CEN ISO/TS 17575-1, CEN ISO/TS 17575-3, CEN ISO/TS 17575-4.

Applicability:

— in-vehicle ITS Station;

— central ITS Station (depending on the particular implementation selected by the Toll Service Provider);

— road-side ITS Station (e.g. for the purpose of blacklists).

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.1.3 Access to sensor data

Requirement: The ITS Station shall ensure access to sensor data which are required by the EFC application.

Remarks / Conditions:

a) The detailed specification of the sensor data depends on the needs of the Toll Charger and Toll Service Provider.

b) The list of sensor data may include but is not limited to:

1) location information;

2) time information;

3) speed information;

4) vehicle class information (e.g. presence of trailer).

Applicability:

— in-vehicle ITS Stations.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider.

#### 7.3.1.4 Access to supporting EFC application data

Requirement: The ITS Station shall ensure access to supporting data which are required by the EFC application.

Remarks / Conditions:

a) The detailed specification of the supporting application data depends on the needs of the Toll Charger and Toll Service Provider.

b) Such supporting data may be available in the in-vehicle ITS Station or in other electronic parts of the vehicle (ECUs).

c) The list of supporting data includes but is not limited to:

   1) vehicle characteristics data (e.g. maximum permissible weight, number of axles, number of seats, emission class, emission data);

   2) vehicle registration data (e.g. licence plate number, vehicle class).

d) The provision of sensor data are subject to their availability to the ITS Station.

Applicability:

— in-vehicle ITS Stations.

Involved roles:

— ITS Station Service Provider;

— vehicle manufacturer;

— Toll Service Provider.

#### 7.3.1.5 Support of toll context data

Requirement: The ITS Station shall ensure access to toll context data required for the use of the toll domain.

Remarks / Conditions:

a) The toll context data shall comply with the rules set out in EN ISO 12855:2012, Clause 6 and Annex A, CEN ISO/TS 17575-3:2011, Clauses 6, 7 and 8 and Annex A, and CEN ISO/TS 17575-4:2011, Clauses 5 and 6 and Annex A.

b) In an interoperable environment the ITS Station shall support toll context data of more than one toll domain.

   1) This requirement does not necessarily require the presence of toll context data for more than one toll domain at a time.

   2) It may require the presences of suitable means and methods which ensure that a minimum set of toll context data are available that ensures the compliant use of the toll domain.

c) Toll Context data may partially be available in other applications or facilities supported by the ITS-S (e.g. digital maps, LDM).

NOTE In EFC toll context data are provided by the Toll Charger to the Toll Service Provider. In this case the responsibility for the availability and correctness of the toll context data are well defined. If toll context data are used from other sources then this responsibility (regarding availability and correctness of the data) needs to be defined and agreed between the involved roles.

Applicability:

— in-vehicle ITS Station;

— central ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider.

#### 7.3.1.6 Access to processing resources and memory

Requirement: The ITS Station shall ensure access to suitable processing, memory and storage resources.

Remarks / Conditions:

a) This requirement involves several aspects:

   1) The EFC application shall get immediate access to the resources at any time. (This may involve access in near real-time.)

   NOTE The exact definition and specification of "near real time" cannot be provided in this TR. It will largely depend on the nature of the toll domain (DSRC vs. GNSS), the particular rules and requirements that apply in this toll domain (e.g. max. duration for the reporting of a passage/use of a Charge Object) and the particular implementation in the in-vehicle ITS-S. A worst case scenario can be found in DSRC based toll domains which typically allow a maximum duration of 100 – 200 ms for a full toll declaration by means of a DSRC transaction.

   2) The ITS Station shall provide processing resources, memory and storage that are capable to run the EFC application tasks with the required performance.

This may involve application priorities (refer also to 9.3.2).

Applicability:

— in-vehicle ITS Station;

— road-side ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.1.7 Access to HMI facilities

Requirement: The ITS Station shall provide access to HMI facilities.

Remarks / Conditions:

a) HMI facilities may either be an integral part of the ITS Station or considered as "external" to the ITS Station (e.g. provided as components of the HMI facilities provided by the in-vehicle electronics).

b) The detailed specification of the HMI facilities required to support EFC applications depend on the rules applying in the respective toll domains(s). Such rules are typically specified by the Toll Charger.

c) HMI facilities may include (non-exhaustive list):

1) means to enable the user to enter tariff determining parameter, like presence of a trailer, number of axles, maximum permissible weight of the actual train, emission class, vehicle class, etc.;

2) means to provide feedback to the users about the actual valid setting of the tariff determining parameters;

3) means to provide feedback to the user about operational status of the EFC application (comprising EFC application itself and then facilities provided by the ITS Station to support the EFC application);

4) means to provide feedback to the user about the status of the payment means related to the EFC Service Contract.

Applicability:

— in-vehicle ITS Station.

### 7.3.2 Security requirements

#### 7.3.2.1 Security and protection of charge data

Requirement: Charge data shall be protected against intentional or unintentional change, manipulation and deletion.

Remarks / Conditions:

a) This requirement shall guarantee that:

   1) the fee charged is correct, and

   2) the charge data can be used as legal prove for the correct collection of fees.

b) This requirement implies that:

   1) only authorized applications get access to the charge data; and

   2) security measures are in place to guarantee the authenticity, integrity and non-repudiation of the charge data.

Applicability:

— in-vehicle ITS Stations;

— central ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider.

#### 7.3.2.2 Privacy of data

Requirement: EFC application data and charge data shall be managed according to the applicable data privacy regulations

Remarks / Conditions:

a) This requirement implies that EFC application data and charge data shall be processed according to Directive 95/46/EC.

b) Not all EFC application data and charge data may fall under this Directive.

c) Certain data privacy rules may vary in different toll domains depending on the applicable national legislation.

Applicability:

— in-vehicle ITS Stations;

— central ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.2.3 Security mechanisms supported by the ITS Station

Requirement: The ITS Station shall enable the EFC application to perform security related functions.

Remarks / Conditions:

a) This requirement implies the availability, access and performance of security functions provided by the ITS Station.

b) The particular security functions in the EFC context depend on the rules and specifications valid in the individual toll domain.

c) Such security functions comprise functions:

d) to check the authenticity and integrity of data received;

   1) to create signatures and authenticators which shall guarantee the integrity and authenticity of data;

   2) to enable secure monitoring.

e) This requirement may involve the need for a dedicated HW, e.g. SAM and/or Trusted Recorder.

Applicability:

— in-vehicle ITS Station;

— road-side ITS Station;

— central ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.2.4 Secure delivery of charge data to the Toll Service Provider

Requirement: The ITS Station shall ensure a secure delivery of charge data to the Toll Service Provider.

Remarks / Conditions:

a) This requirement relates to the provision of captured/processed charge data from the EFC application to the Toll Service Provider.

b) Such data provision involves functions and services outside the control of the EFC application.

c) This requirement also relates to functions provided by services that are outside the ITS Station (e.g. the network services that connect ITS Stations to each other).

d) It is assumed that the Toll Service Provider has to comply to minimum requirements regarding security functions involved and the level of expected security.

e) Such security functions may comprise:

   1) delivery of the charge data using a secured communication channel (which prevents unauthorized access to the data);

   2) means to ensure authenticity, integrity and non-repudiation of charge data.

Applicability:

— in-vehicle ITS Station;

— road-side ITS Station;

— central ITS Station.

Involved roles:

— ITS Station Service Provider;

— Communication Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.2.5 Support of secure monitoring and trusted recorder

Requirement: The ITS Station shall support the use of EFC specific security functions “Secure Monitoring” and “Trusted Recorder”.

Remarks / Conditions:

a) The applicability of such functions depends on the individual toll domain.

b) Depending on the capability and the architecture of the EFC application such functions may (partially) be integrated in the EFC application.

c) The functions are specified in Draft ETSI/TS 120 814 (Secure Monitoring), and in a future specification in regard to the trusted recorder.

Applicability:

— in-vehicle ITS Station;

— road-side ITS Station;

— central ITS Station (requires a trusted recorder).

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.3 Operational requirements

##### 7.3.3.1 Life cycle management for the EFC application

Requirement: The ITS Station shall enable a life cycle management of the EFC application at any time while it is activated in a toll domain.

Remarks / Conditions:

a) This requirement implies:

   1) Access to the EFC application for management proposes shall be guaranteed.

   2) A suitable communication channel shall be made available (for in-vehicle ITS Station at least when it is inside the corresponding toll domain).

   3) The Toll Service Provider (for an EFC application on an in-vehicle ITS-S) or Toll Charger (for an EFC application on a road side ITS-S) shall be in the position to change, update, delete, activate or deactivate the EFC application.

   4) Rules and processes are in place which enable such life cycle management involving the C-ITS System Operation.

b) It is assumed that hardware components are not covered by this requirement as for such hardware different requirements may be applicable.

   NOTE The life cycle and the respective management of hardware components of an (in-vehicle) ITS-S significantly differs from the life cycle management of software components and is very closely connected to the life cycle management of the vehicle itself. It is outside of the scope of this TR.

Applicability:

— in-vehicle ITS Station;

— road side ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.3.2 Management of EFC application data

Requirement: The ITS Station shall enable a management of EFC application data.

Remarks / Conditions:

a) This requirement implies:

   1) Access to the EFC application data shall be guaranteed at any time.

   2) A suitable communication channel is made available (for in-vehicle ITS Station at least as long as it is inside the corresponding toll domain).

   3) Toll Service Provider and / or Toll Charger shall be in the position to change, add or delete EFC application data.

   4) Rules and processes are in place which enables such management involving the C-ITS System Operation.

b) EFC application data may e.g. comprise:

   1) context data (autonomous EFC charging application);

   2) contract / user data;

   3) various lists (EFC enforcement application).

Applicability:

— in-vehicle ITS Station;

— road side ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

#### 7.3.3.3 Configuration of the EFC application

Requirement: The ITS Station shall enable configuration of the EFC application.

Remarks / Conditions:

a) This requirement implies:

   1) Access to the EFC application shall be guaranteed at any time.

   However, priorities of ITS applications shall be considered (it is expected that EFC does not get the highest priorities amongst all ITS applications).

   2) A suitable communication channel is made available (for in-vehicle ITS Station at least as long as it is inside the corresponding toll domain).

   This has also an impact on functions outside the (in-vehicle and road side the ITS Station as it requires a suitable communication channel being provided by a network service and the availability and capability of the corresponding central ITS Station.

   3) Rules and processes are in place which enable such management involving the C-ITS System Operation.

Applicability:

— in-vehicle ITS Station;

— road side ITS Station.

Involved roles:

— ITS Station Service Provider;

— Toll Service Provider;

— Toll Charger.

# 8 EFC services in the C-ITS environment

## 8.1 EFC services on ITS Stations

In order to ensure the operation of charging system using an EFC solution several services need to be available. Those services which are of importance from the perspective of this Technical Report are:

— EFC charging service (DSRC mode);

— EFC charging service (autonomous mode);

— EFC enforcement service;

— EFC location support service.

NOTE ISO 17573 specifies EFC as one single service comprising all required functionalities like charge object detection, data capturing, charging, enforcement, billing, reporting and others. For the purposes of this Technical Report, this single EFC service is split into several services which in total enable EFC.

The Service User of the EFC charging service is the Road User. This service basically detects the use of a toll liable piece of the road infrastructure, captures all tariff determining parameters (e.g. vehicle class) and thus enables a calculation of a toll fee due.

In contrast, the Service User of the EFC enforcement service is the Toll Charger. The detection of a vehicle using a toll liable piece of the road infrastructure serves as input for this service. The result of the enforcement service is the provision of data which enable a decision if a user of a toll liable vehicle behaves compliant to the rules of the toll regime. It furthermore provides required data to start a legal enforcement action (that may finally result in sanctioning such incompliant behaviour).

The EFC services may require more than one application in order to provide the envisaged service result (refer also to the definition of the term “application” as provided in prCEN ISO/TS 17427). Furthermore in the context of the communication architecture in C-ITS an application is considered as an association of two or more complementary ITS-S applications (see [ETSI EN 302 665]).

In order to provide the above listed services the following applications are required on ITS Stations.

To enable an autonomous EFC charging service the following applications are required:

— autonomous EFC charging application on an in-vehicle ITS-S;

— autonomous EFC charging application on an central ITS-S (optional proxy part);

— location augmentation application on a road side ITS-S (optional).

To enable a DSRC based charging service the following applications are required:

— DSRC based EFC application on an road side ITS-S;

— DSRC based EFC application on in-vehicle ITS-S.

To enable an enforcement service the following applications are required:

— compliance checking application on an road side ITS-S;

— compliance checking application on in-vehicle ITS-S.

## 8.2 Involved C-ITS sub-roles in the life cycle of EFC services

### 8.2.1 Life cycle of EFC services

The entire life cycle of EFC services can be divided into the following phases:

— preparation phase;

— development phase;

— deployment phase;

— operation phase;

— end of life phase.

Figure 14 outlines these phases and provides examples which major tasks or actions are involved in the individual phase.

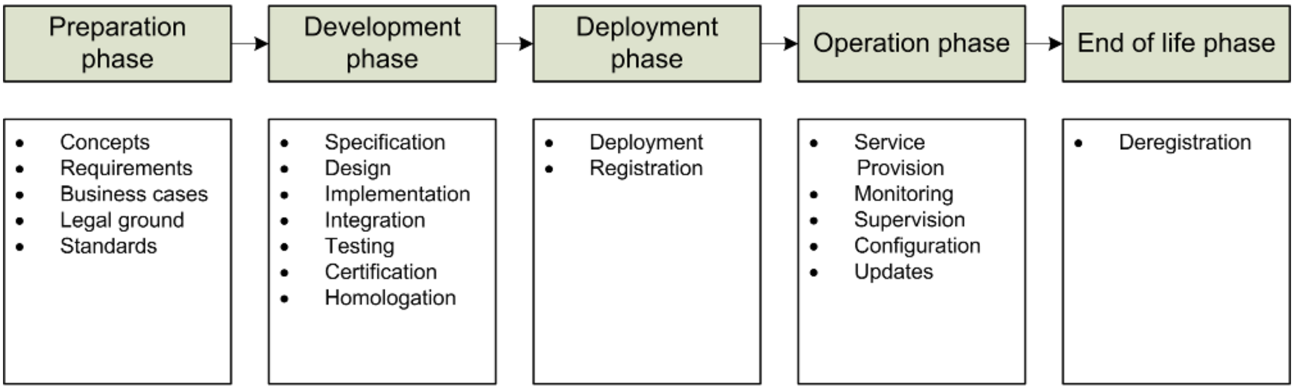



**Figure 14 — Life cycle phases of EFC services (and examples of major tasks)**

The *preparation phase* usually starts with a business idea and business decision. After base concepts and the applicable legal base are evaluated the necessary technical, operational and legal pre-requisites for the services will be prepared respectively provided. Furthermore, available standards may support in this phase to provide detailed specification and design work in the next phase. However, also the creation of the necessary legal ground (initiating new legislations or changes in existing laws) as well as creating of useful standards may be required.

In the *development phase* detailed specifications (technical specifications, operational processes) are provided. Based on these specifications the applications enabling the envisaged services are designed, implemented and tested. Integration activities may be required on different integration levels. Final acceptance testing (including end-to-end tests and operational service trials) give evidence about the compliance of the system and process implementation to the requirements and the suitability of the applications in an operational environment. In many cases certification and homologation is required to conform to legal requirements.

The objective of the *deployment phase* is to make the services and applications available to the system and to register the services. The services and applications are made available to the target / production platform at the end of this phase.

The *operation phase* is determined by the daily operation of the service with the agreed (guaranteed) performance level. Thus monitoring and supervision task belong to the daily operation. Optimization of the service or adaptation to a changed environment may be achieved by a life cycle management. Such life cycle management comprises e.g. parameter changes, changes in system configuration and even deployment of new updated versions of the applications.

At the *end of the life* of a service, the service will be deregistered and the applications will be removed from the production platforms.

### 8.2.2 C-ITS sub-roles involved in different phases of the EFC service life cycle

#### 8.2.2.1 General

In case EFC services are provided on ITS Stations the roles and sub-roles which are available in C-ITS environment shall guarantee the support of EFC services in each phase of the service life cycle.

The following subclauses and tables provide information which C-ITS sub-roles (refer to prCEN ISO/TS 17427 and 5.2.1.2) are involved in the individual phases of the entire life cycle of EFC services.

#### 8.2.2.2 Preparation phase

In the preparation phase only sub-roles of the role Policy Framework are involved. As in this phase no C-ITS related technical and operational tasks are carried out, no sub-role from System Management and System Operation are required.

In the very early stages of this preparation phase C-ITS roles do not necessarily get involved in the activities. Possible business ideas and concepts for EFC services may be carried out by existing or potential Toll Charger or existing or potential Toll Service Providers without the need for C-ITS specific knowledge and know-how.

The involved sub-roles shall mainly support in providing the ground for the envisaged EFC service. This ground mainly consists of legal and technical regulations that need to be considered or prepared in order to operate the planned service.

Depending on the particular EFC service (see 8.1) on the EFC stakeholder side either the Toll Charger (road side enforcement services, road side DSRC charging services) and/or the Toll Service Provider (in-vehicle enforcement services, autonomous charging service and in-vehicle DSRC charging) are active.

**Table 1 — C-ITS sub-roles involved in the preparation phase**

| **EFC service related tasks** | **C-ITS roles (sub-roles)** | | | |
|---|---|---|---|---|
| | **Policy Framework** | **System management** | **System operation** | **Using the system** |
| Preparation of concepts and requirements, business cases | - | - | - | - |
| Assessment of the legal ground | Legislation, jurisdiction<br>Policy institution | - | - | - |
| Involvement of existing standards or provision of new standards | Standardization organization | - | - | - |

#### 8.2.2.3 Development phase

In the development phase sub-roles of the System Management get involved. In this phase the sub-roles ensure that the services are designed, implemented and tested in a way that C-ITS related aspects (like resource sharing, operational and technical conditions and limitations) will be taken into account already in a very early stage of the process.

Testing, certification and homologation activities will again involve sub-roles from the role Policy Framework. Such certification and homologation activities may be optional in other C-ITS services. However, EFC services require the complicate to the particular certification and in most cases in addition to national homologation rules.

**Table 2 — C-ITS sub-roles involved in the service development phase**

| EFC service related tasks | C-ITS roles (sub-roles) | | | |
|---|---|---|---|---|
| | **Policy Framework** | **System management** | **System operation** | **Using the system** |
| Preparation and provision of specifications (technical and operational) | Compliance Manager,<br>Security Certification Body | Project Manager, C-ITS Architect,<br>Service Owner,<br>Risk Manager | - | - |
| Implementation | - | Project Manager | - | - |
| Integration work | - | Project Manager | - | - |
| Testing (including end-to-end testing and operational service trials) | - | Project Manager,<br>Test Manager | - | - |
| Certification | Compliance Manager<br>Security Certification Body | Project Manager,<br>Test Manager | - | - |
| Homologation | - | Project Manager,<br>Test Manager,<br>Homologation Manager | - | - |

#### 8.2.2.4 Deployment phase

In this phase the services and related applications will be deployed to the production C-ITS environment. This deployment will be performed under the responsibility of the C-ITS role System Management and requires involvement of all sub-roles of this role.

After successful deployment the services will be registered in the C-ITS service catalogue. From that point in time the EFC services are made available to the service users upon their request.

**Table 3 — C-ITS sub-roles involved in the service deployment phase**

| **EFC service related tasks** | **C-ITS roles (sub-roles)** | | | |
|---|---|---|---|---|
| | **Policy Framework** | **System management** | **System operation** | **Using the system** |
| Deployment and registration | - | Service owner,<br>Service catalogue manager,<br>Communication manager | - | - |
| Service Provision (to the target/production platform) | - | Access Manager,<br>Capacity manager,<br>Communication manager | - | User |

#### 8.2.2.5 Operation phase

Both roles System Management and System Operation are involved in the operations phase. Daily operational tasks are characterized by monitoring and supervision activities. In particular service levels – which play an extremely important role in the provision of EFC services – require close and real-time monitoring and immediate reporting.

Typical IT life cycle management (application configuration and updating) is carried out in order to keep the services and applications adapted to changes of the C-ITS system and the technical and operational environment as well to implement changes in the EFC services.

**Table 4 — C-ITS sub-roles involved in the service deployment phase**

| **EFC service related tasks** | **C-ITS roles (sub-roles)** | | | |
|---|---|---|---|---|
| | **Policy Framework** | **System management** | **System operation** | **Using the system** |
| Monitoring and supervision | - | Service owner,<br>Service level manager<br>System monitoring<br>Financial manager | Content provision,<br>Service provision,<br>Presentation provision | User |
| Configuration, Updates deployment | - | Technical analyst,<br>Change manager,<br>Configuration manager,<br>Capacity manager | - | - |

#### 8.2.2.6 End-of-life

The service owner initiates the end of life of the concerned service. The service and related applications will be deregistered, deleted from the C-ITS service catalogue and finally removed from the C-ITS production platform. Operational processes will be suspended. The sub-roles of the role System Management ensure the activities in this phase.

**Table 5 — C-ITS sub-roles involved in the end-of-life activities**

| **EFC service related tasks** | **C-ITS roles (sub-roles)** | | | |
|---|---|---|---|---|
| | **Policy Framework** | **System management** | **System operation** | **Using the system** |
| Deregistration (and removal from the production platform) | - | Service owner<br>Service catalogue manager | - | User |

## 8.3 Combined models of EFC services in C-ITS context

### 8.3.1 C-ITS and EFC role model relations

In C-ITS the roles and responsibilities are based on an organizational architecture viewpoint represented by four major roles. On the sub-role model level a set of required technical and organisational functionalities (see 8.2) for each role (except for using the system role) is defined. The EFC role model on the other hand is more an actor representing role model not detailing the organizational architecture viewpoint of the roles. prCEN ISO/TS 17427 describes C-ITS as a system and the roles occurring in this system, the roles are independent from the implementation of a service on an ITS Stations. In contrast the EFC view makes a clear distinction between the role and actor who is responsible for the OBE - the in-vehicle ITS-S - and the RSE – the road side ITS-S. For that reason a direct mapping of C-ITS and the EFC role model is not possible.

Figure 15 shows the role model relations – the relation between the EFC actor roles and C-ITS organisational roles - for two of the three use cases for an EFC implementation on ITS Station based environments. These are the role model relations regarding the required EFC services on an

— road side ITS Station; and

— in-vehicle ITS Station.

The third use case regarding the central ITS Station for an EFC system relates to TSP and TC back offices. This use case is not shown because these are most likely TC and TSP proprietary implementations using either the complete ITS Station architecture or only its communication stack. It is assumed that these instances of central ITS Stations will only run the EFC back office service, but no other ITS service will reside in this EFC dedicated back office.

Figure 15 shows on the right side the EFC role model and mostly on the left side the ISO C-ITS organizational architecture represented by the four major roles. The upper part of the figure shows mainly the road side and the lower part the in-vehicle ITS Station to relation to EFC.

The two ITS Stations are most likely be operated by different independent entities in an interoperable EFC system, only the Policy Framework role will be implemented by the same stakeholder (comparable to the EFC System Management role) for both ITS Stations for the EFC system. To illustrate this assumption, three of the four organisational roles from the C-ITS model are shown double in Figure 15. This allows illustrating which role of the EFC role model is connected to which C-ITS role depending on the responsibility for the corresponding ITS Station.

A first major difference between the ITS-S types is the different EFC role for the C-ITS “Using the system” role. For the road side ITS-S the EFC Service User is the Toll Charger as for the in-vehicle ITS-S the EFC Service User is the road user.

The second main and important difference is the service owner. For the road side ITS-S it is the same as the Service User, the Toll Charger. The Toll Service Provider is the EFC service owner of the in-vehicle ITS-S.

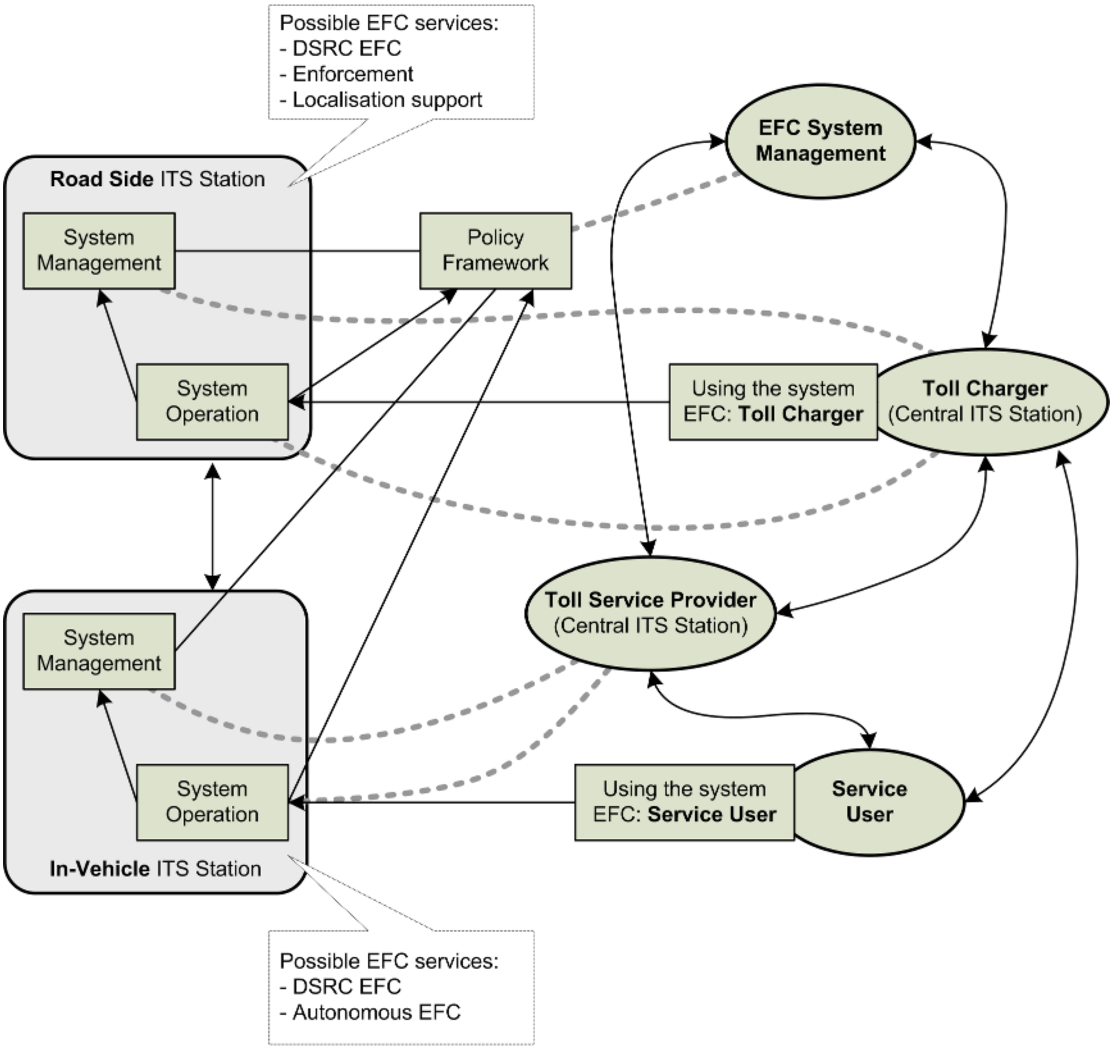



**Figure 15 — C-ITS and EFC role model relations**

The dotted lines in Figure 15 are indicating the EFC role actors taking responsibility for the C-ITS major roles. It is important to understand that this does not mean the EFC actor covers the whole set of sub-roles represented by the C-ITS major role.

The EFC System Management supports or incorporates most or the entire C-ITS Policy Framework sub-roles, which are identical for the road side and the in-vehicle ITS-S regarding the EFC application. For the Toll Charger and the Toll Service Provider it is, besides who is the service owner, not so clear which sub-roles of the C-ITS System Management and System Operation are assigned to them and which are assigned to other actors of the C-ITS environment (in-vehicle ITS-S and road sided ITS-S service provider). The decision about the responsibilities for the C-ITS sub-roles has to be made by an agreement of the stakeholders implementing and operating the systems and services.

### 8.3.2 Technical EFC architecture in C-ITS context

For the technical EFC architecture in C-ITS context it is important to understand how the provisioning of the ITS and EFC services has to be done. The provisioning process is defined in 5.3.3. Figure 16 shows the provisioning of the EFC services and applications using an ITS-S service provider. The TSP or TC are developing or buying the EFC service and providing these services and applications via the Host Management Centre to the target ITS Station.

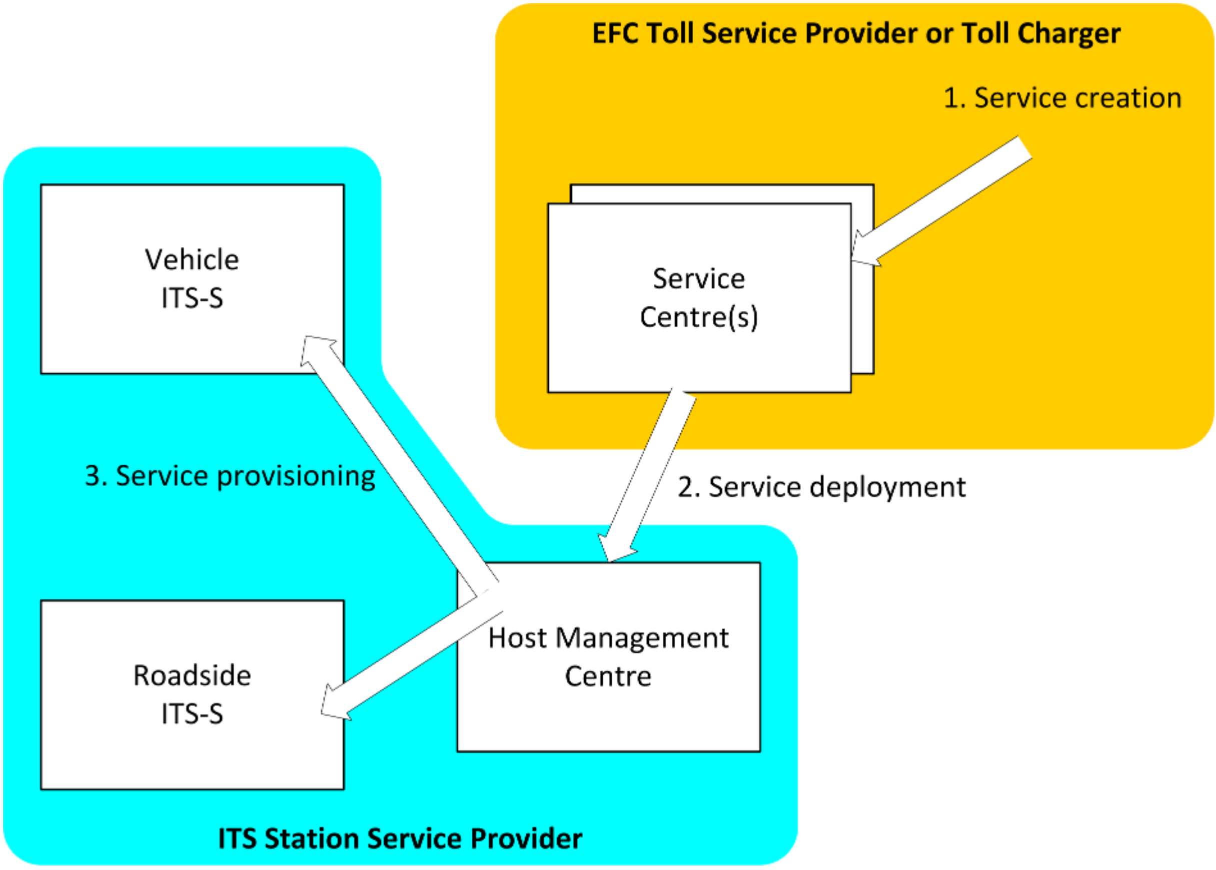



**Figure 16 — Application provisioning with ITS Station Service Provider**

Based on the findings of the EFC and C-ITS role model relations and the application provisioning process shown in Figure 16, the technical EFC architecture in a C-ITS context can be developed. The architecture is based on the EFC architecture overview figure in 6.3.1. The RSE is now the road-side ITS Station and the OBE is the in-vehicle ITS-S. To adapt the C-ITS context into the EFC role model two new roles shall be added:

— road side ITS Station Service Provider;

— in-vehicle ITS Station Service Provider.

The role ITS Station Service Provider is not equal to the ITS specific role Service Provisioning. The ITS-S Service Provider may cover a part of the tasks and responsibilities allocated to the role Service Provisioning.

Details with respect to the definition of the ITS-S Service Provider role and the relationship of this role to the ITS specific roles like Service Provisioning and System Operation are provided in 8.3.3.

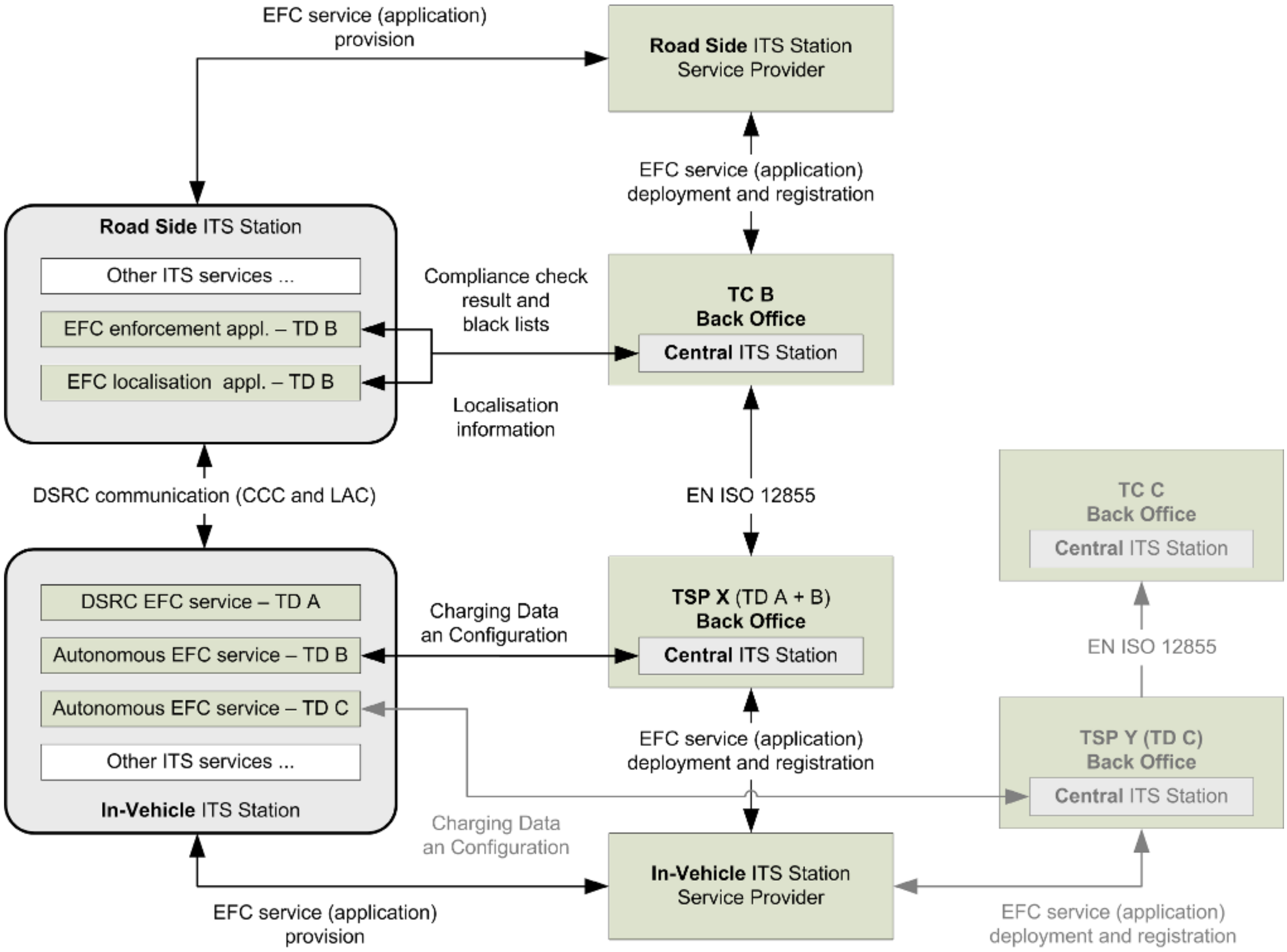



**Figure 17 — Example technical EFC architecture in C-ITS context**

Figure 17 shows an example of the technical architecture for a toll domain B (TD B) with an autonomous OBE approach. The Toll Charger B uses a road-side ITS Station Service Provider located in his TD B for the required road side EFC services enforcement and localization support (LAC). TC B has accepted Toll Service Provider X for the EFC service provision on an in-vehicle ITS Station in his toll domain.

In a first step, the EFC services are deployed and registered by the ITS Station Service Provider and in a second step provided to the ITS Stations. Application or service updates during the system operation will be done using the same distribution path. A direct communication between the service on the ITS Station and the service owner (TSP and TC) without passing the ITS Service Provider as shown in Figure 16 might be possible in some cases but is not mandatory.

But TSP X is accepted in toll domain B as service provider, and offers in addition a DSRC solution for toll domain A. TSP X has an agreement with an in-vehicle Service Provider for the deployment and provision of its EFC services for TD A and TD C. In the example this in-vehicle ITS Station Service Provider has also an additional agreement with TSP Y for the toll domain C EFC service.

Of course both the road side ITS-S as well as the in-vehicle ITS-S may operate several additional ITS application or services in parallel.

### 8.3.3 ITS Station Service Provider

The new ITS Station Service Provider (ITS-S SP) role required for the definition of an extended EFC role model in a C-ITS environment is responsible for all sub-roles of the C-ITS organisational role System Management, except the service owner sub-role. The ITS-S SP is not directly involved in the System Operation sub-roles. The ITS-S SP is just responsible for the availability of the ITS-S, its maintenance, etc. during the operational phase of the EFC service.

On the other hand, just looking on the ETSI ITS Station architecture (without any C-ITS organisational role model aspects) the ITS Station Service Provider is the role providing an ITS Station supporting the parallel execution of different ITS services. The ITS-S SP is responsible for the hardware and the basic software platform (e.g. the operating system) to be used by one or more ITS services.

The ITS-S SP is from an EFC point of view a provider of a multi-application ITS platform allowing the execution of a dedicated and possibly interoperable EFC application. The EFC application or service is developed either by the TSP or the TC depending if it is an in-vehicle or road side ITS-S.

### 8.3.4 Extended EFC role model in C-ITS environment

When trying to adapt the C-ITS approach into a role model as used for the EFC role model, the introduction of ITS Station Service Provider roles as mentioned in 8.3.2 is required. There are possible other roles in the C-ITS model but for EFC only the ITS Station Service Provider roles are relevant. In an extended EFC role model for C-ITS each kind of ITS Station could have an own service provider role as shown in Figure 18.

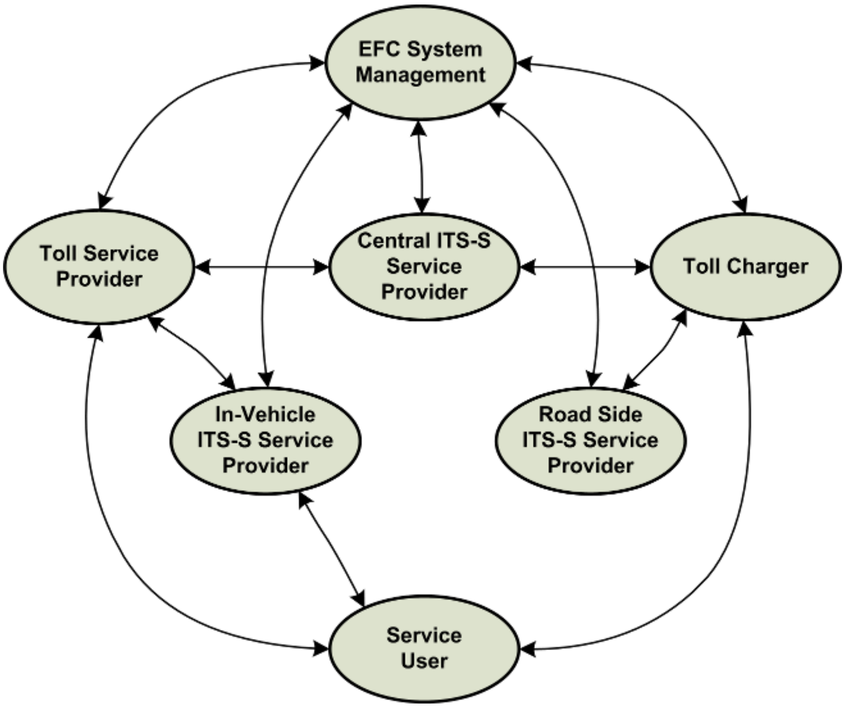



**Figure 18 — Extended EFC role model with three ITS-S service providers**

This principle role model is also applicable in case a mixed environment is present. There are several alternatives for mixed environments possible. Examples are:

— in-vehicle ITS-S with on EFC application and dedicated EFC RSE which do not apply the ITS-S architecture;

— dedicated EFC OBE (no ITS-S architecture) and EFC applications on in-vehicle ITS Stations in one toll domain.

Reflecting these options for mixed environments in a more abstract approach only one ITS Station Service Provider role is required. This ITS-S Service Provider role is deploying one or all ITS Stations required in an EFC system. This model is shown in Figure 19.

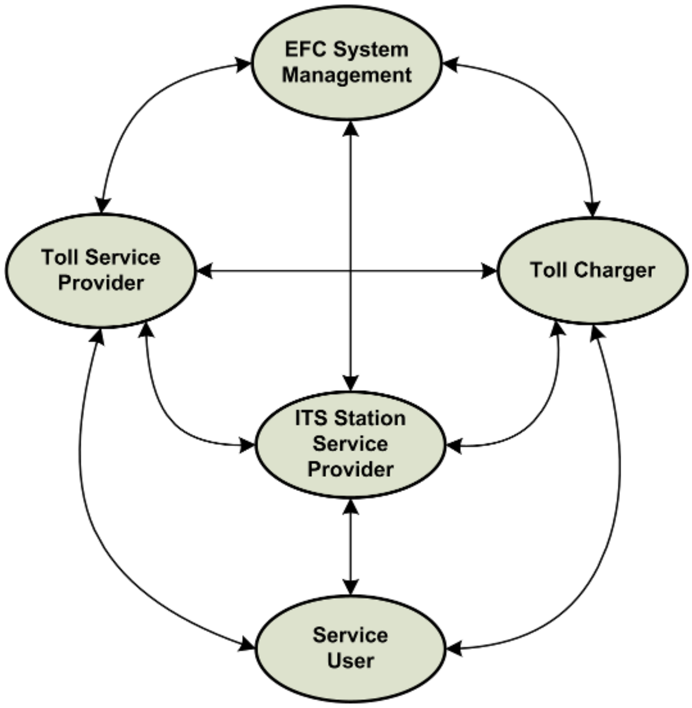
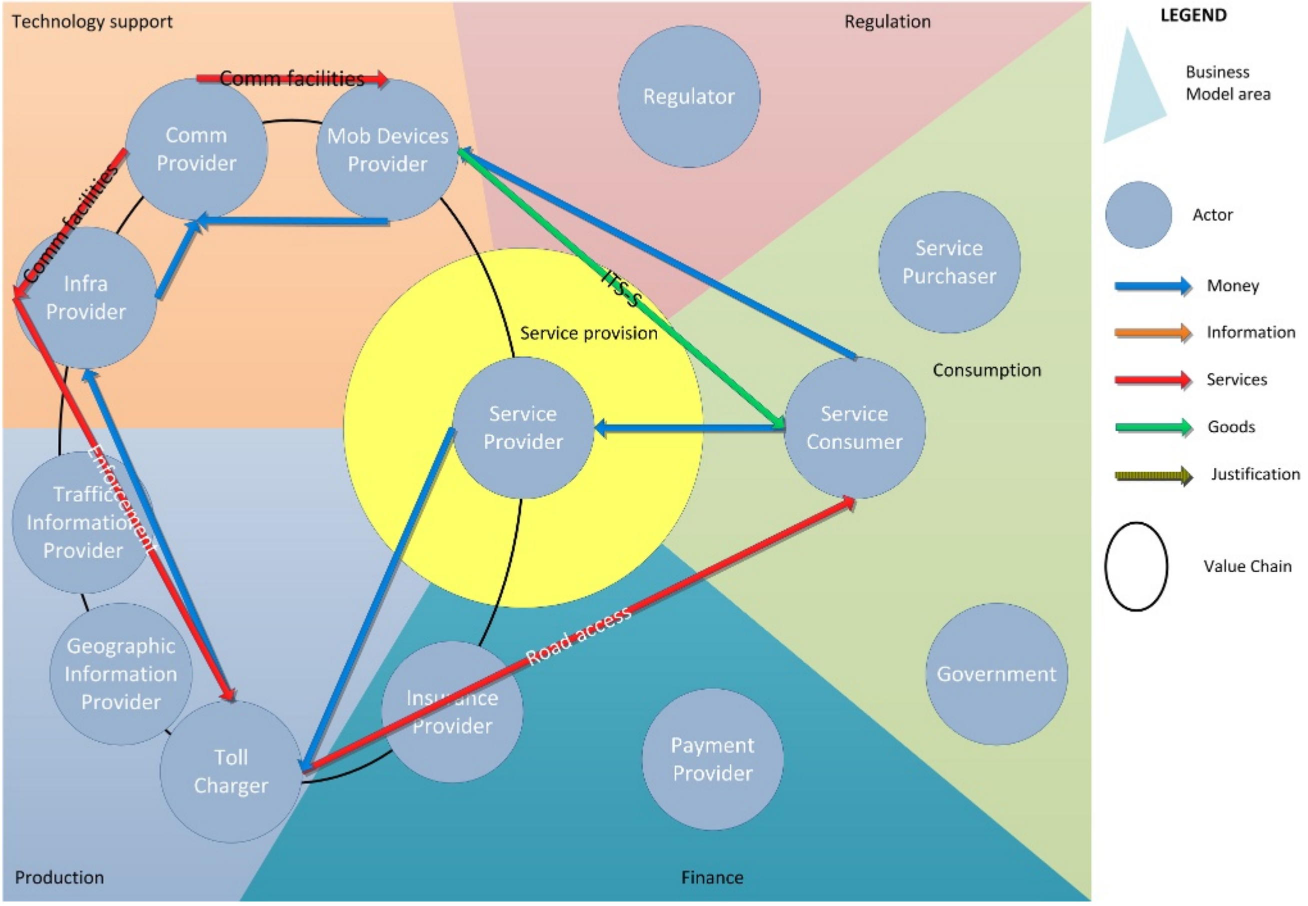



**Figure 19 — Extended EFC role model with single ITS Station service provider role**

The role models in Figure 18 and Figure 19 assuming that the functional C-ITS role “Policy Framework” and its sub-roles are realized by the EFC System Management as far as they are required for the EFC system implementation.

### 8.3.5 Business architecture

Based on the conceptual business model template from CVIS (see Figure 4) the EFC service running on top of a C-ITS can be modelled:




The above figure should be seen as an example. Other options are possible. Only major interactions between the involved actors are shown.

**Figure 20 — Example conceptual business model for EFC in an C-ITS system**

In this model the Service Provider is equivalent to the Toll Service Provider. The Service Consumer is the service user/road user (which in most cases is the same as Service Purchaser). The model assumes that the Service Consumer owns the in-vehicle service platform, as illustrated by the green arrow from Mob Devices Provider to Service Consumer. The Infra Provider is providing required infrastructure to the Toll Charger to do enforcement tasks and localization support. Both the Toll Charger and the Service Consumer consume communication services, but in the model it is assumed that Infrastructure Provider and Mobile Devices Provider, respectively, act as a “broker” towards the Communication Service Provider. It can also be foreseen a model where Toll Charger and Service Consumer buys these services directly from the Communication Service Provider.

# 9 Considerations on particular implementation aspects

## 9.1 Introduction

An open ITS Station architecture with a core platform would enable “plug-and-play” integration of both regulatory and commercial applications (see Figure 17). With this modular approach, additional functionalities could be progressively integrated for areas like safety, sustainability, efficiency and comfort using a common platform with a joint HMI. This modular approach especially suits the market for ITS applications for heavy vehicles, as this market is extremely fragmented. No single application is assumed to create significant benefits for a large segment of the market. Especially in the freight sector the need of different vehicle operators differ widely, dependent on the nature of the transport task they offer. However, note that road charging is a sensitive application in the sense that Toll Chargers are not prepared to take any risk of losing revenue by complications arising from other applications competing for on-board resources. So it is of major importance that the charging application runs in a “clean” environment.

The multi-application ITS Station can be designed around the concept of core and application specifications (refer also to CEN/TR 16219). The core specifications focus on the requirements that are common across multiple applications. For example, the requirements around the technology to determine the location of the vehicle/ITS Station would be considered as core specifications. Application specifications focus on the requirements of a particular application. For example, a digital tachograph application would include requirements regarding the recording of working hours. Separating the specifications into core and application specifications allows for incremental specifications of future applications. It is envisaged that a new application will draw upon as much of the functionality contained within the core requirements as possible. The additional functionality will be described in the application specifications. The concept of core and application specifications can be compared with a regular PC. The PC contains a core set of programs to allow it to operate, which can be considered as the output of a core specification. Programs that can be loaded onto the PC, such as Microsoft Word, may be thought of as being the output of an application specification.

## 9.2 Synergies

The integration of both regulatory and commercial applications on an open ITS-S has several benefits in addition to the potential cost savings and reduced clustering of the driver environment. It also enables the different applications to use the same information (coming from the facilities layer (see ETSI EN 302 665)) or allow them to directly exchange information with each other. This integration and information reuse can provide enhanced ease of use and/or increased service levels. From an EFC viewpoint such integration can for example result in:

a) automatic setting and update of variable toll parameters (e.g. loaded weight, no. of axles, presence of trailer…);

b) use of actual tolling tariff in navigation service;

c) re-use of payment functionality/facilities:

   1) micropayment means can be provided by the facilities layer of ITS-S;

   2) EFC contract/means of payment used for paying other services;

d) enforcement functionality can be used by other applications, e.g. AVI/ERI or other authority required applications such as implementation of low emission zones;

e) use of emission class for toll charge computation – possible as used in low emission zone application.

It should be noted that direct exchange of information between different applications on the same ITS-S requires careful versioning of all involved applications. Small changes in the behaviour of one application might affect other depending applications. In general the facilities layer will be more stable and reuse through a rich facilities layer is preferred (governed by the core specifications as outlined in 9.1).

An ITS-S with a feature rich facilities layer enables very light weight applications, reducing complexity and cost for application development. The facilities for application provisioning and life cycle management enables these applications to be installed (and possible uninstalled) on demand. From an EFC viewpoint this opens new possibilities regarding interoperability of tolling where the base for interoperability is a well-defined facilities layer, and area local applications are installed on demand for each toll domain. Such an approach allows local EFC services which are fully adapted to the local condition. It might also allow introduction of EFC in areas where the current standards are considered too limited.

Another benefit from deploying EFC applications on an ITS-S is the availability of V2I and V2V communication facilities at 5.9GHz. These V2I and V2V communication facilities can be used for both CCC and LAC. Compared to traditional communication means for CCC and LAC, i.e. CEN DSRC or infrared DSRC, V2I and

V2V at 5,9 GHz provide better communication ranges and is also less sensitive to non-optimal antenna/transponder placements. Especially in the case where moving vehicles are used for CCC this can be a mayor benefit. However, particular attention needs to draw to the need to unambiguously identify the particular vehicle from which CCC data are retrieved (in order to not penalize road user which correctly pay the required toll fees).

## 9.3 Particular and critical areas in relation to EFC in an ITS environment

### 9.3.1 Phase of migration from dedicated EFC devices to ITS-S based EFC

To date EFC is solely based on in-vehicle equipment which is dedicated to EFC (EFC OBE). The nature of such equipment varies – depending on the charging technology applied in the respective toll domain – from self-powered DSRC OBE which is fitted to the windscreen to more complex OBE for GNSS/CN toll domains requiring connection to permanent vehicle power supply.

This situation will change after first EFC services are available on in-vehicle ITS-S. This phase is determined by a mixed availability of both types of EFC implementation types - dedicated EFC OBE and EFC application on in-vehicle ITS-S (see Figure 21). In general such mixed environment is not a problem as long as it can be guaranteed that per vehicle only one EFC application is active per toll domain.

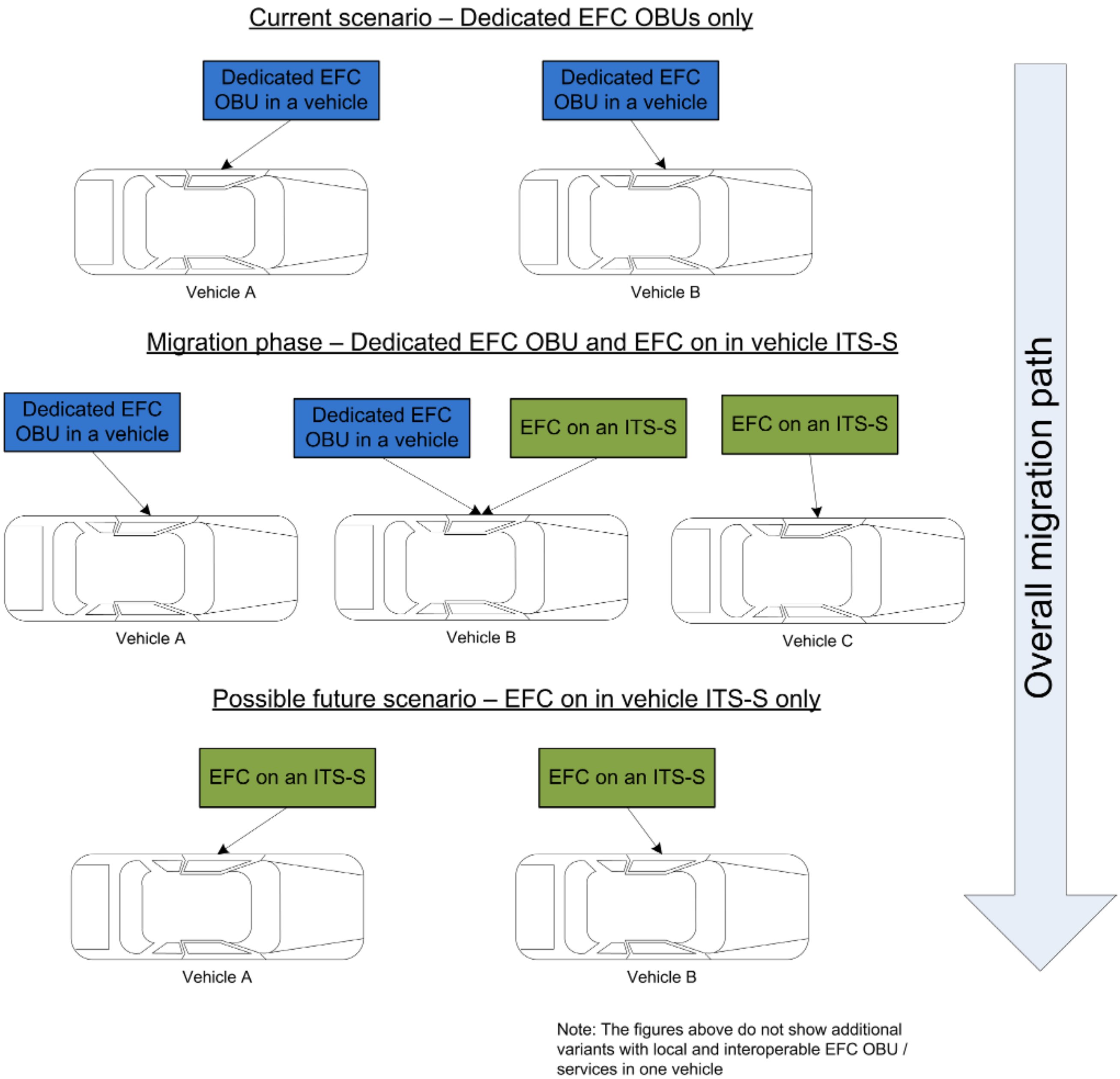



**Figure 21 — Overview on migration phases from dedicated EFC in vehicle equipment to EFC on ITS-S**

Major challenges in the entire migration process can be expected in the phase in which both, dedicated EFC OBU and EFC services in ITS in-vehicle stations are available. Once EFC services on ITS in-vehicle platforms are made available different scenarios with respect to already existing EFC OBE that are present in the same vehicle can apply (see Table 6).

In the optimum case the following steps are to be taken by the involved stakeholders:

— EFC Service User contacts his ITS Station Service Provider or the Toll Service Provider in order to establish an EFC service contract and to get the EFC application enabled on the ITS Station available in the vehicle.

— The EFC Service User removes the dedicated EFC OBE from the vehicle before the EFC services on the ITS Station is available.

— The EFC Service User returns the dedicated EFC OBE to the Toll Service Provider for deactivation.

This scenario ensures the presence of only one active EFC OBE / application in the vehicle per toll domain. However, other scenarios will happen and need particular consideration (see Table 6).

**Table 6 — Scenarios in the EFC migration phase**

| Scenario | Presence of EFC OBE / EFC application in the vehicle | Toll Service Provider | Coverage of toll domains | Major Problem |
|---|---|---|---|---|
| A | - EFC OBE available<br>- EFC service on ITS-S not activated | | | None. |
| B | - EFC OBE removed<br>- EFC service on ITS-S activated | | | None. |
| C | - EFC OBE available<br>- EFC service on ITS-S activated | - EFC service contract with one or more than one Toll Service Provider | - non-overlapping coverage of individual toll domains | None. |
| D | - EFC OBE still available<br>- EFC service on ITS-S already activated | - EFC service contract signed with one Toll Service Provider only | - overlapping coverage of toll domains | Risk of double charging. See explanation below. |
| E | - EFC OBE still available<br>- EFC service on ITS-S already activated | - EFC service contract signed with two different Toll Service Providers | - overlapping coverage of toll domains | Risk of double charging. See explanation below. |

In *Scenarios A and B* do not provide any problem Only one EFC application (EFC OBU based or EFC application on ITS-S) is active at a time.

In *Scenario C* the EFC Service Contacts are non-overlapping, i.e. they provide active EFC Service in different toll domains.

*Scenario D* applies in case an EFC Service User who currently uses a dedicated EFC OBE migrates to an EFC service on an ITS-S but keeps his EFC service contract with the same Toll Service Provider in place. In this case the EFC Service User should return the EFC OBE to the Toll Service Provider. In case he does not return the OBE the Toll Service Provider should prevent the possible generation of double EFC transactions (one generated by the EFC OBE, the second generated by the EFC application on the ITS-S). Toll Service Providers have different options to avoid such double transactions:

— remotely disabling the EFC OBE (in case the OBE supports such remote configuration interface);

— blacklisting the EFC OBE (this requires the involvement of all Toll Chargers of toll domains for which the EFC service contract is valid and may lead to unwanted and unjustified enforcement actions against the EFC Service User);

— detection of double transactions and deletion of the one produced by the EFC OBE (this may involve the Toll Charger of the toll domain in which this transaction was generated);

*Scenario E* is a case in which the ITS-S Service Provider does not offer an EFC-service with the same Toll Service Provider to which the EFC Service User already has a contract. In such a case EFC Service User may

— keep the existing contract with the Toll Service Provider and establish the new (ITS-based) EFC contract for different toll domains only (then Scenario C in Table 6 applies), or

— create a new EFC Service Contract and fully cancel the existing contract one (then Scenario B in Table 6 applies).

If the service user takes none of the above two measures, then there is the risk of generation of double transactions. Both the EFC OBE and the EFC application on the ITS-S produce toll transactions independently from each other. There is no chance for the two involved Toll Service Providers to identify and avoid such double charging. The EFC Service User should notice the problem with the next invoices.

The following rules should prevent problems in the migration phase and can be used as guidelines:

— Non-overlapping coverage of toll domains by different in vehicle EFC equipment does not lead to problems and potential mistakes in charging.

— Both Toll Service Provider and ITS-S Service Provider shall provide necessary information to the EFC Service User about risks and impact of potential use of both dedicated OBE and EFC applications on ITS-S in one vehicle.

— Toll Service Provider should implement and support processes which identify potential double transactions generated by both the EFC OBE and the EFC application on an ITS-S for the use of the same charge object by the same vehicle. Double transactions should not lead to double charging (= one of the two transactions should not lead to charging).

It should be further noted that the challenges which occur in the migration phase are similar to those which are expected in interoperable EFC environments. In such environments local contracts (supported by locally enabled OBE) and interoperable contracts (supported by interoperable OBE) may also be present at the same time in one vehicle.

It is important to emphasize that depending on the particular technical implementation of the ITS-S (single OBE host/router, multi OBE host/router) (refer also to 9.5.3) in an interoperable environment the above outlined scenarios may provide particular and additional challenges. As an example a scenario with two EFC services on one ITS-S shall be mentioned. One of these EFC services may related to a local contract covering one particular toll domain only, whereas the second EFC service may be an interoperable EFC service which covers multiple toll domains.

### 9.3.2 Resource management

All ITS applications residing on an in-vehicle ITS-S share the same resources that are available at this platform. It can be expected that resources like:

— storage capacity;

— memory space;

— processing capacity;

— access to and bandwidth of interfaces (including communication channels)

are limited on such ITS-S. There are various reasons for limited resources like cost optimization, outdated C-ITS HW- and SW-platforms in vehicles or others.

On the other hand there may be ITS applications available on in-vehicle ITS-S which provide different types of services, ranging from time critical emergency and safety-of-life services via public regulated services, information services to pure infotainment and entertainment services. Such multiple ITS applications on one ITS-S typically make use of the same (limited) resources and therefore may influence each other. The Technical Report ETSI/TR 102 638 provides a first overview on such applications and has also identified initial requirements – amongst others - in respect to:

— system capabilities; and

— system performance.

The following sub-requirements in these two main areas are of particular interest in relation to EFC applications on in-vehicle ITS-S:

a) System capabilities:

1) radio communication capabilities (e.g. radio communication channels being used);

2) network communication capabilities (e.g. congestion control and message priority management);

3) vehicle absolute positioning capabilities (e.g. GNSS capabilities);

4) vehicle communication security capabilities (e.g. respect of privacy);

5) other vehicle capabilities (e.g. vehicle interfaces to sensors).

b) System performance:

1) vehicle communication performances (e.g. maximum round trip delays);

2) vehicle positioning performances (e.g. absolute position accuracy);

3) vehicle communication system reliability and dependability performances (e.g. radio coverage);

4) security operation performances (e.g. signing and verifying messages and certificates).

Typical requirements in EFC applications in the above mentioned two areas are:

— CN based radio communication capabilities (e.g. GPRS, EDGE, 3G and 4G) in GNSS based toll domains;

— 5,8 GHz based radio communication capabilities (according to the relevant set of CEN TC 278 standards) in DSRC based toll domains;

— satellite based localization capabilities (e.g. GPS, Galileo/EGNOS, GLONASS) in GNSS based toll domains;

— autonomous power supply capabilities (if no vehicle power supply is available) in order to ensure the possibility to provide compliance check data at a parking ground;

— secure data and security credential storage capabilities (e.g. DES, 3DES, AES-128… according to the requirements of the respective toll domain);

— time-to-first-fix (TTFF) performance in GNSS based toll domains (e.g. 1 min) in order to ensure a detection of Charged Objects immediately after the start of a journey;

— security credential processing performance (e.g. DES-CBC-computation in 3 ms) in order to ensure checking and creating of access credential and authenticators in real time and limited communication zones.

It has to be noted that such requirements are toll domain specific to a large extent.

In general it is the task of the management plane on the ITS-S to manage the access to resources for all applications residing on the ITS-S. Such management is based on *application priorities*. An example method for priorities in terms of access to communication media is specified in ISO 21218. The basic concept is that every resource user (= application) when requesting access e.g. to a communication medium shall provide the parameter *user priority*. Based on this parameter the Communication SAP will allocate the required medium.

With respect to application priorities EFC services are considered as publically regulated services. As a consequence in the context of ITS services EFC applications are not in the group of applications with highest priority.

NOTE Time critical road safety applications are expected to get the highest priority level amongst the different ITS services.

Therefore it is expected that there will be cases in daily service provision in which the EFC application on the ITS-S does not get the required resources in order to fulfil the EFC services with the expected minimum level of performance.

EXAMPLE In a DSRC based toll domain the exchange of data with an EFC road side equipment can only take place in small zones (e.g. up to 10 m) at particular locations. If the vehicle passes such a zone and at exactly the same point in time the ITS-S processes a critical road safety application such data exchange with the EFC road side equipment may not be guaranteed. As a result the vehicle may pass the EFC road side equipment without having provided toll declaration Data. As a consequence such vehicle / EFC Service users may be identified by the Enforcement services operated by the Toll Charger as toll violator.

In order to prevent unjustified legal actions against the EFC Service User in case of such events an exception handling should be implemented. The following minimum requirements are recommended:

a) logging of the exceptional event (including date/time, location, reason) by the management plane of the ITS-S;

b) provision of information regarding the exceptional event to:

   1) EFC Service User (e.g. by means of the HMI indication the non-performance of the transaction);

   2) ITS-S Service Provider (e.g. by the management resources on the ITS-S);

   3) Toll Service Provider (either by monitoring functions included in the EFC application and/or by the ITS-S Service Provider); and

   4) Toll Charger as part of the data provided in compliance checking communication;

c) the further processing shall be done according to the rules applicable in the respective toll domain (e.g. generation and provision of an alternative set of toll declaration data for the missed charge object by the Toll Service Provider or use of an alternative method of payment for the use of the charge object by the EFC Service User.

### 9.3.3 Performance monitoring

The area of performance plays a major role in EFC services. The need to ensure a maximum level of toll income for the owner of the road infrastructure has led to a framework of performance requirements and performance related contracts in EFC services.

In order to achieve such maximum level of toll income typically several performance based contracts are in place between the entities carrying out individual roles and tasks:

— contract between the Toll Charger and the entity or organization that operates the toll system (if such operator is existing as a separate entity);

— contract(s) between the Toll Charger and the Toll Service Provider(s);

— contracts(s) between the Toll Charger (respectively the acting operator) and supporting subcontractors.

Such contracts define key performance requirements, KPI, respective bonus / penalty schemes, but also liabilities for damages that may be a result of non- or reduced performance in certain areas.

Typical contractual performance requirements are:

— compliance with contractual milestones;

— minimum performance levels of toll charging processes (there are several variants and sub-performance figures known), also known as under- and overcharging;

— minimum performance levels of enforcement processes (also split into sub-performance figures);

— minimum performance levels of Road User related services (e.g. call centre performance, waiting time at point of sales).

It is expected that entities and roles which will be involved if EFC is deployed over C-ITS will also be part of such performance based contracts. This will in particular concern the ITS-S SP. It is expected that the ITS-S SP needs to enter into performance based contracts with the Toll Service Provider(s) which deploys EFC services via the ITS of the ITS-S SP. Such contracts may relate to:

— minimum operational availability level of the in-vehicle ITS-S;

— maximum time for repair or replacement of a malfunctioning in-vehicle ITS-S.

As C-ITS provides a complex environment, involving several different players and entities like hardware providers, software providers, platform operators, provider of non-EFC services and communication service providers, that are all using the same platform, the need for monitoring of performance on the in-vehicle ITS-S is evident.

EXAMPLE 1 An EFC application that resides on an in-vehicle ITS-S is not able to detect and report the use of a Charge Object (e.g. virtual toll point in a GNSS based toll domain) in the required minimum period of time as the access to the CN-communication stack was blocked due to a malfunction in a infotainment application on the same platform.

EXAMPLE 2 An EFC application that resides on an in-vehicle ITS-S is not able to transmit toll charge data to a road side station in a DSRC based toll domain, as at the time of passage of the DSRC RSE the management plane of the ITS-S allocated all processing and memory resources of this C-ITS to a time-critical road safety application.

In both examples the road user may suffer from receiving a fine for non-compliant behaviour on a tolled road. In addition the EFC Service Provider may not reach the target levels he agreed with the Toll Charger for charging performance which may lead to significant penalties

These examples show the need for a facility (module or dedicated function) that is capable to monitor the proper functioning and level of performance of the EFC application on the in-vehicle ITS-S. Such facility may not be able to improve the performance, but it should:

— log events of improper performance (including date/time information, major system states, error codes...);

— provide such data to the EFC Service Provider;

— provide an input to processes in the EFC application that ensure the information to the road user about the proper functioning of the EFC application; and

— provide an input to the EFC enforcement application in order to provide status information to an enforcement body by means of a compliance check communication.

It is expected that many C-ITS applications will use such performance monitoring facilities – either as an integral part of the individual ITS application or as a supporting application. An alternative solution is the use of performance monitoring facilities provided by the ITS-S (e.g. function in the operating system of the ITS-S).

As data which are captured, logged and transferred by such a facility will be used to solve disputes (potentially involving financial liabilities) such performance monitoring facilities may have to undergo a dedicated certification process.

## 9.4 Suitability for use and certification

### 9.4.1 Introduction

The certification and suitability for use process is required to enable the trust of a Toll Charger into the charging data collection process of an EFC service running on an ITS Station. There are two different levels of complexity for the certification and suitability for use test:

— single toll domain EFC service;

— interoperable EFC service, for example as required by EETS.

For a single toll domain EFC service the certification and suitability for use test can be done based of one single EFC system specification, moreover the certification authority might be the Toll Charger of the toll domain. In an interoperable EFC system like EETS this process will be much more complex. Either the EFC service shall be certified and tested according to individual rules of each Toll Charger of the interoperable system (this seems to be the approach in EETS) or all Toll Chargers have agreed on one or more certification and test authorities, applying identical certification and test procedures.

NOTE Information on suitability for use tests is not completely included in currently available EETS toll domain statements. If information on suitability for use tests is provided, the details of the procedures are not publicly available, but disclosed to an EETS Provider after signing a non-disclosure agreement, for example.

Figure 22 shows the certification and suitability for use procedure in alignment on the procedure defined in Annex 4 of “Guide for the application of the directive on the interoperability of electronic road toll systems” (EETS application guide). This procedure is applicable and will cover the whole ITS Station with the EFC service. A recertification is required in case if essential changes in the EFC service. A big question mark shall be set on what is defined as an “essential change” because an ITS Station may host several different applications including the EFC application. Such an essential change may be defined as

— an essential change in the EFC service;

— an essential update of the ITS Station operating system or basic software;

— adding another service/application to the ITS Station; and/or

— an essential change of another application running on the ITS Station.

It has to be expected that the Toll Charger(s) will define about the nature of such an "essential change" and it is most likely (due to known problems with similar multi-application platforms like PC and smart phones) that it will include any major change (as listed above) of the ITS Station configuration (for more information see 9.5) that will initiate the need for recertification.

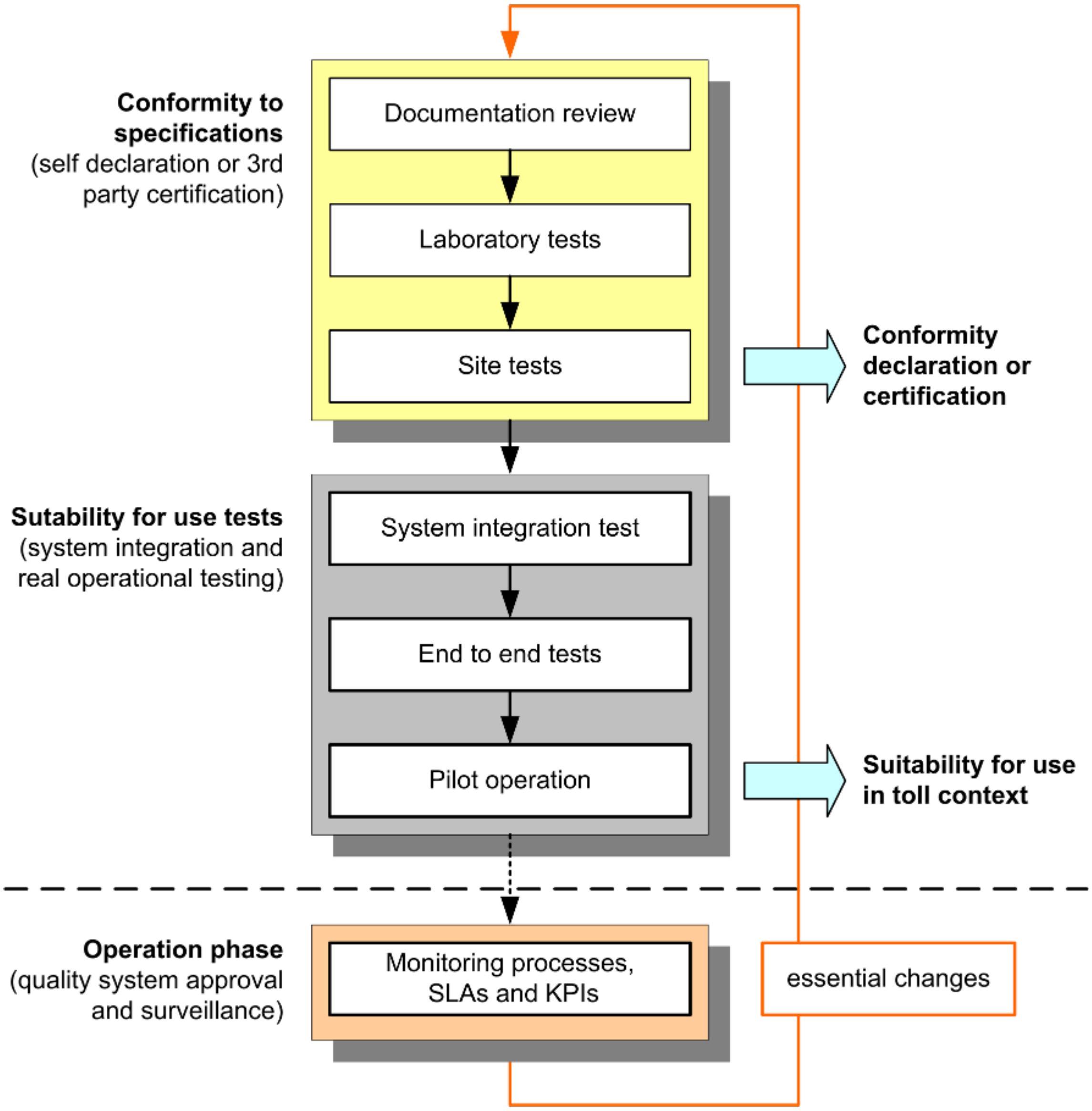



**Figure 22 — Certification and suitability for use procedure**

### 9.4.2 Conformity to specifications

The conformity to specification declaration contains the CE certification of the ITS Station to all relevant standards with the conformity statements (in EETS the notified body's certificate) including the evaluation report(s) and the detailed test reports. It contains also the conformity declaration to the Toll Chargers EFC requirement specification.

The complete conformity to specification declaration that has to be provided to the Toll Chargers shall be delivered by the ITS-S manufacturer and/or the ITS Station Service Provider and the EFC Service Provider.

### 9.4.3 Suitability for use tests

The suitability for use tests covers all aspects of charging data collection, back office data exchange, performance and service level agreement monitoring as well as security and privacy issues. The suitability for use test phase is divided into the following sequence of test steps:

1) system compatibility tests (e.g. ITS-S with EFC service laboratory tests and tests at the test site, back office interface tests in a test environment);

2) end to end tests with the ITS-S in the operational EFC environment (= Toll Charger(s) environment);

3) pilot operation phase with a limited time and number of ITS Stations.

This test steps are ideally performed in cooperation between Toll Charger, ITS Station Service Provider and the EFC Service Provider. However, the responsibility for the test phase remains with the EFC Service Provider.

### 9.4.4 Certification

Certification might be used as a supplemental or alternative procedure to parts of the process shown in Figure 22. As mentioned above, certification of equipment will simplify the test procedure in an interoperable environment. Certification instead of a suitability for use test has to be preferred especially if a Toll Charger or EFC Service Provider has a lack of knowledge in the C-ITS environment, which is not knowing the impact of other C-ITS services to the EFC service. In case of an interoperable EFC environment or lack of knowledge the certification process can be outsourced to or supported by a certification authority (which may be a Notified Body, e.g. in case of EETS).

Generally, certification refers to the confirmation of certain characteristics of an object, person or organization. In this Technical Report certification applies to:

— the ITS Station;

— the EFC application; and

— the EFC Service Provider processes

for which requirements need to be formulated. These requirements should be described as tests to be passed. Each requirement should lead to a verdict (passed or failed) on which the certification is based. For example, consider the IP code that classifies the degrees of protection provided against – amongst others – water in electrical enclosures, which provides more detailed information than vague marketing terms such as “waterproof”. The requirements can be directly defined as test cases. It is, however, also possible to first define the requirements on a functional level and then define them as test cases. The advantage of the second way is that first agreement on the functional requirements can be sought, before reformulating these requirements as tests to be passed.

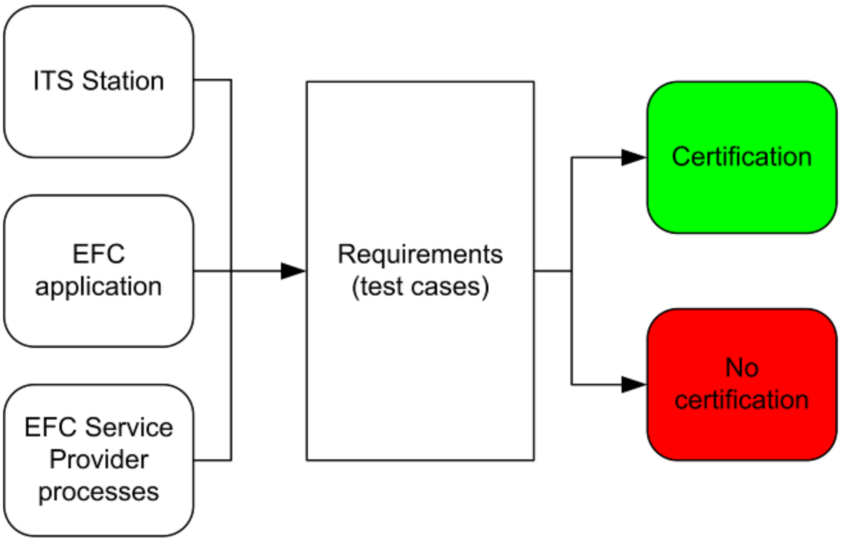



**Figure 23 — Requirements as test cases for certification of ITS Station, EFC application and Service Provider**

The first type of certification is the certification of the ITS Station. This refers to processes intended to determine if the ITS Station and its corresponding equipment (e.g. software) meets the functional requirements, the minimum standards to ensure the required quality for EFC and other ITS applications.

Existing standards and specifications developed by different international standardization bodies set out only conceptual requirements for the ITS Station architecture and their communication interfaces. Real functional, technical and quality requirements allowing the implementation of a multi-application ITS Station cannot be found in such standards. A complete set of requirements is also theoretical impossible, because this would assume that every future application had been involved in the requirements analysis.

Due to the fact that there is currently and also in future no detailed and complete set of requirements for a generic ITS Station, the certification of a generic ITS Station as a first step is also not possible. Therefore the first step is to certify the ITS Station against the set of EFC application requirements on an ITS Station as set out in 7.3 in this Technical Report.

The certification of an EFC service/application for a specific ITS Station is based on the detailed requirements for the charging data collection defined by a Toll Charger or in an interoperable EFC system the requirements from all involved Toll Chargers.

Certification of EFC Service Provider processes will also include requirements for the organization. For example, an organisational requirement can be related to a minimum turnover of X EUR per year. Note that such requirements should not be too narrow, as positional providers should not be excluded too easily. Other requirements, such as financial backing and business plan, are in this respect important as well. Process requirements refer to the IT system used in, for example, the collection, processing, data storage, data reporting, security and quality management procedures.

### 9.4.5 Registration and Certification Authority

The ITS Station reference architecture defined by ISO 21217 refers to a registration authority as a basic means to enable secure maintenance. The function is to register ITS applications and related messages at an ITS registration authority, and to restrict access to “Facilities”, “Management” and “Security” dependent on the rules as defined by the ITS registration authority. Every ITS application class/ITS application shall be therefore uniquely identified by an application identifier in order to be handled in ITS Communications.

In ETSI EN 302 665 only a registration authority is mentioned. But a more important task of a similar authority – a certification authority - will be certifying all components of the ITS Station; the basic hardware and operating system, the services and communication stack as defined in ETSI EN 302 665, the EFC application and Service Provider processes as outlined in 9.4.4.

It is mentioned as a note in ETSI EN 302 665 that more than one single registration authority may exist. But only one registration and certification authority should be responsible for one ITS Station and the applications executed by this host.

#### 9.4.6 Quality system approval und surveillance

- **Key performance indicator (KPI) and service level agreement (SLA):**

In the operational phase of an EFC system the quality system approval and surveillance shall be performed by the Toll Charger(s). This is measuring the KPI and calculating the reached SLA. So far there is no difference compared to a system with a dedicated EFC OBE. But in fact there is a two level SLA. The first SLA is between Toll Charger and EFC Service Provider and second between the EFC Service Provider and the ITS Station Service Provider. It is not assumed that the Toll Charger has a contract with the ITS-S SP and measuring its KPI and SLA, this is the task for the EFC Service Provider (refer also to 9.3.3).

The conclusion is that the Toll Charger set up a requirement to the EFC Service Provider to have a SLA with the ITS-S SP ensuring the SLA defined by the Toll Charger.

- **Auditing:**

It is recommended to recertify the EFC Service Providers after a certain period of time. This evaluation is generally called audit. Audits are performed to ascertain whether the certification is still valid. This also applies to the ITS Station and EFC application: it shall be ensured that the certified ITS Station and EFC application are still being used unchanged. Relevant changes of the ITS Station or EFC application shall be announced by the ITS-S SP and/or EFC Service Provider and auditing is only performed to force them to behave according to this obligation. The EFC application and/or ITS Station need recertification in case of major changes.

The auditing process is an important and powerful tool for quality system approval and surveillance.

NOTE The most useful approach in auditing is not only a go/no go decision, but to think along with the EFC Service Provider and support to further develop the business and thus the EFC scheme. It goes without saying that the auditing process needs clear criteria related to potential damage to the EFC scheme (e.g. loss of money).

### 9.5 Governance and responsibility

#### 9.5.1 Introduction

There are two dimensions regarding governance and responsibility of an ITS Station and its applications.

First, it is assumed that a single ITS Station will provide a variety of ITS applications, both commercial and regulatory. This distinction between commercial and regulatory applications is not made by the basic set of ITS applications defined in ETSI/TR 102 638 but this is the most important difference regarding governance and responsibility of the regulatory EFC application. In the commercial landscape, it is already common to see ITS technology supporting multiple software applications. For example, one in-vehicle device may incorporate route guidance, engine monitoring, speed monitoring, etc. Analogous to the commercial landscape, it is envisaged that regulatory ITS applications (e.g. EFC, e-Call, etc.) will further be released to improve efficiency and safety in road use. The current task is to analyse and provide guidance on the issues of governance and responsibility for a regulatory EFC application running in parallel with other – commercial and/or regulatory – applications on the same ITS Station.

The second dimension of the governance and responsibility question is the technical implementation of an ITS Station and the distribution of the EFC service/applications to one or more OBE hosts (see Annex B of ETSI EN 302 665 V1.1.1 (2010-09)).

An in-vehicle ITS Station may consist of more than one OBE host and OBE router.

#### 9.5.2 Application configuration of the ITS Station

On one hand, interoperation may be the core feature of an ITS Station to create a multi-application environment. It can be defined as the ability of a system to exchange services with other systems. There are two different kinds of interoperation. Vertical interoperation is the integration of different applications of the same kind, for example the interoperation between the existing DSRC based motorway tolling systems and a future GNSS based EFC system for a whole country. Horizontal interoperation allows exchange of data and services between different applications on the same platform, for example sharing the same basic vehicle and trip data. On the other hand, an ITS Station may only provide the same resources (basic services, sensor inputs, communication channels) to different applications without allowing them sharing of application dependent services and data. This is a multi-application environment. But also a mixed approach of applications with interoperation and pure parallel executed applications is possible.

Figure 24 illustrates three investigated ITS Station configurations for interoperation or as multi-application environments with respect to EFC applications on ITS Stations:

— Regulatory ITS Station: This ITS Station is based on horizontal interoperation or multi-application environment and contains only mandated regulatory applications. A certification entity installed by law will certify all applications or the whole ITS Station.

— Tolling and charging ITS Station: This ITS Station is based on vertical interoperation or multi-application environment and contains only charging and tolling applications, be it a mandatory EFC application or the various existing private road tolling systems. The ITS Station and the regulatory charging application will be certified. The additional interoperable functionality for the existing DSRC motorway tolling systems might require a different acceptance procedure which could be organized under private commercial rules.

— Multi-application ITS Station: The possible interoperation of this ITS Station is based on both horizontal and vertical integration. The ITS Station is a standardised platform designed to support all conceivable road-related applications (the basic set of ITS applications). Certified regulatory applications run in parallel with possibly not certified, not audited commercial applications.

The three configuration areas may be seen as overlapping governance areas with different governance and responsibility priorities.

An additional approach for an ITS Station application configuration is:

— Closed ITS Station: An ITS Station may only allow the installation of certified applications of any kind. If the number of certified applications is low, possibly each combination of applications is also checked during the certification process. This means that under any circumstance each requirement of each application will be fulfilled. But such an approach is very expensive because of the huge number of test cases during the certification even with a very small number of certified applications.

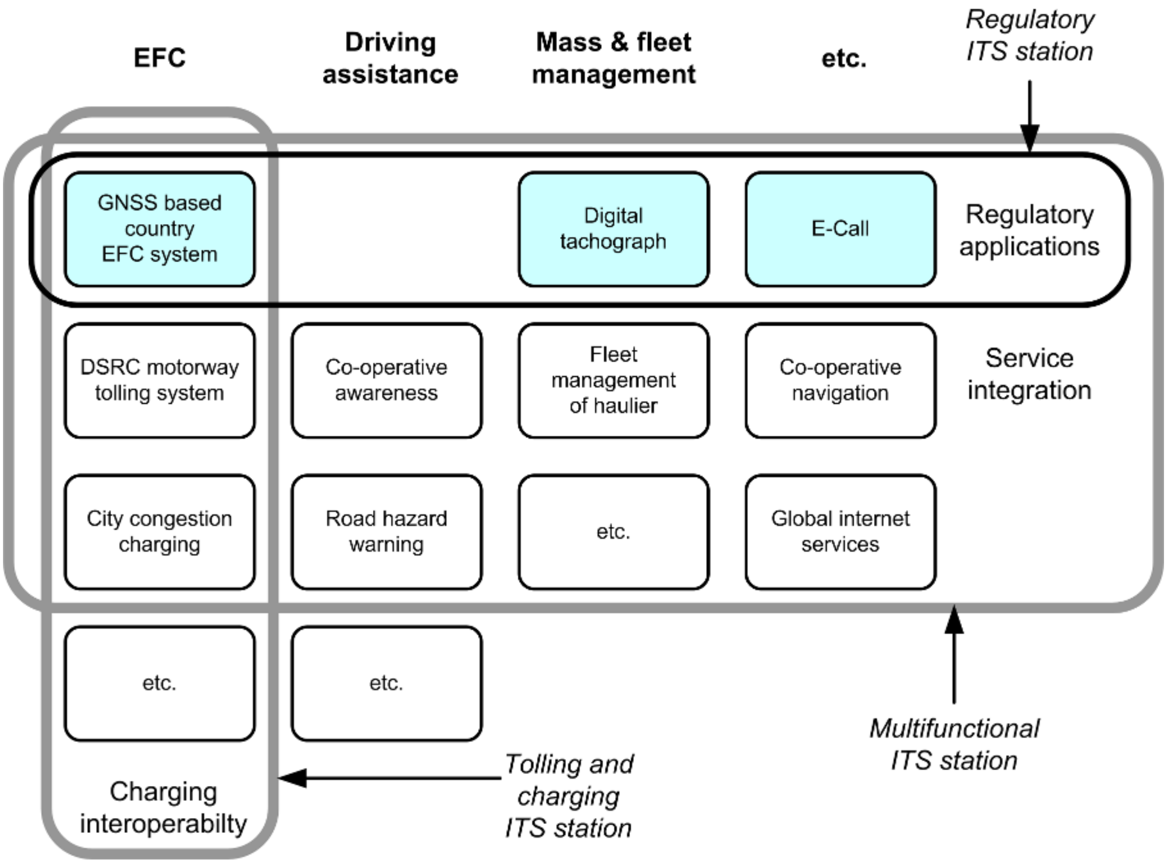



**Figure 24 — Configurations of an ITS Station**

### 9.5.3 Technical implementation of the ITS Station

#### 9.5.3.1 General

The ITS communication architecture outlines several in-vehicle ITS Station implementations with different complexity levels. The two most different ITS Station implementations are:

— single OBE host / router (ETSI EN 302 665 V1.1.1 (2010-09), Figure B.3: Small vehicle implementation);

— multi OBE hosts and routers (ETSI EN 302 665 V1.1.1 (2010-09), Figure B.1: Advanced vehicle implementation).

The single OBE host / router implementation is from the technical approach comparable to a dedicated EFC OBE, except the fact that the supported applications are not limited to EFC. The multi OBE host / router is a combination of several identical and/or different OBE hosts and routers communicating with each other using an in-vehicle network (IVN).

#### 9.5.3.2 Single OBE host / router

In a single OBE host / router implementation the EFC application has to share all resources (the central processing unit, memory and other resources) with all other application and services installed on the ITS Station. It shall be strongly assumed that for such a small ITS Station in short and mid-term only the “regulatory ITS Station”, the “Tolling and charging ITS Station” and the “closed ITS Station” approaches will guarantee the required SLA and KPI requirements defined by the Toll Charger in any circumstance. Adding other not tested and certified applications (e.g. an entertainment application) on such single OBE host / router might lead to situations in which the SLA will not be fulfilled.

The most significant advantage is the cost reduction arising from sharing a single hardware amongst several applications while using of synergies between the various applications, which are most likely delivered by the same ITS Station Service Provider. The single OBE host / router multifunctional ITS Station also allows a simple managed approach what information the driver receives or what input is required. This is a significant safety benefit for the driver, who only interacts with one device rather than having many devices competing for their attention at the same time.

#### 9.5.3.3 Multi OBE host / router

The configuration with the lowest number of remaining technical and organisational issues is a multi OBE host and router implementation, the EFC application has its own OBE host without any other application using it. In such an implementation the EFC application receives all required sensor input from the in-vehicle and/or ITS Station-internal network. Communication with the EFC Service Provider back end has to be done with an OBE router which provides its service to several OBE host and application. This can be seen as the only bottle neck, especially in case of a thin client EFC implementation. Such an implementation approach – EFC application on its own OBE host – supports every of the application configurations described in 9.5.2 is possible. There remaining issues to be solved are

- guarantee of in-vehicle communication network availability;
- sharing of most likely only one user interface with a huge number of other applications;
- provision of required OBE router availability for communication with the EFC service provider back end.

#### 9.5.3.4 Other OBE host and router configurations

Between the single OBE host/ router and the multi OBE host and router other combinations with any shade of grey between are possible, but do not provide any significant advantage. For example distribution of parts of the EFC service on different OBE host will only increase the solution complexity for development and testing.

#### 9.5.3.5 Virtualisation of the host environment

An additional approach to reduce issues between different C-ITS services running on the same platform is a virtualised environment for each service on an ITS Station. These are protected runtime environments for the simultaneous and secure execution of different services and application. That means there is no data exchange on the service level. The different services use only the same input, facilities and communication media. The idea is the same as described in 9.5.3.3 having a single, but only virtualised host for the EFC service. More information on such concepts can be found for example on the OVERSEE project homepage (http://www.oversee-project.com).

### 9.5.4 Update and installation of applications

#### 9.5.4.1 General

Although a multi-application environment has significant benefits, it is also important to consider the complexity that this concept introduces. A multi-application environment will require regular updates to the applications, which may introduce errors or faults to other applications (e.g. these applications might suddenly no longer operate). This is also valid for the “regulatory ITS Station” and the “closed ITS Station” approaches if the new configuration is not tested properly.

Also the introduction of new applications shall be carefully managed. Each new application will require resources of the ITS Station, such as memory to operate or bandwidth on the communication network. It is important that the storage requirements of the old applications are not compromised as to affect their original function. Furthermore, when introducing new applications, care should be taken with respect to uploading viruses or other malicious programs which may affect the operation of the whole ITS Station.

Therefore, continually managing the functionality and operation of a multi-application ITS Station is an on-going task, to be merely performed by the ITS Station Service Provider and the registration and certification authority. The ITS Station Service Provider should be responsible for the design, development and testing of the applications on the ITS Station and the continued monitoring of the ITS Stations performance. The certification authority should be responsible for approving the introduction of new applications to the ITS Station based on information provided by the ITS Station Service Provider, the application owner and independent verification testing.

#### 9.5.4.2 EFC thick client versus thin-client concepts

An EFC application running on an ITS Station can be implemented in a thick client or thin client architecture, with potentially any possible mixed scenario between the thick and thin extremes (see 6.3.3).

In the EFC thick client approach, most parts of the data processing steps are performed on-board the in-vehicle ITS-S. Also the largest parts of all other applications are installed on the ITS Station. However, the update and maintenance processes for all applications are difficult to manage. With several applications side by side, and possibly different ones in different vehicles, it is hard to guarantee that EFC and regulatory applications run in a “clean” environment.

In the EFC thin client approach, a significant part of the data processing steps are performed in the back-office. Raw data are sent to the back-office and processed centrally using application software. EFC and most or all other applications use the same raw data in the back office, with time and position information being the most important ones. Adding applications does not or only in unusual cases require additional software to be installed on the ITS Station. Some applications might require some data storage capacity or other functionality on-board (e.g. in case of immediate driver feedback) at the ITS Station. Nonetheless, updating and installation of these small application parts are practicable processes. So the maintenance of an EFC thin client approach is much simpler for a multi-application environment.

## 10 Guidelines for further work

### 10.1 Role of EFC to boost the deployment of C-ITS

It is broadly expected that first ITS services which will be made available to road users are in the area of road user safety. Also the public area (e.g. European Commission) and automotive manufacturers heavily support activities in this strategic direction. Such services can be easily integrated into already existing driver assistances functions like emergency braking support.

A second area of applications that may be amongst the first applications for commercial deployment are information services which improve the efficiency while using the roads. Example applications are in-vehicle signage and signal phasing and timing. Such applications are seen attractive and beneficial from the road user perspective and thus may lead to a fast spread on the market.

Despite EFC is not amongst these two areas of preferred and “day-one” ITS applications it is expected that EFC will even leverage the deployment of ITS-platforms and thus support the fast deployment of other ITS services. Main reasons for this are:

— a significant part of the road users are already familiar with EFC;

— EFC is mandatory for some vehicle classes (e.g. trucks) on a large proportion of the road network that is commonly used by this type of vehicles (toll domains typically cover the entire highway network in several countries, e.g. in Germany, Poland, Austria, Spain, Italy and France, and provide interoperable services in a multi Toll Charger environment – also in a cross-border context, like in France and Spain);

— ITS caters for better integration of services and required hardware (replacement of the dedicated EFC OBE);

— EFC provides a large customer base (that may be used to market other applications);

— more toll schemes (supported by EFC) will be made available in the next years and decades throughout Europe, thus EFC provides for an increasing and reliable business for service providers;

— future EFC toll schemes will increasingly cover larger road networks and thus ask for more GNSS based tolling technology. For such technology the benefits of an integration into an ITS platform are more evident compared to existing EFC technology;

— cost savings are expected for Toll Service Providers (as no dedicated hardware is required).

Based on these reasons it is expected that in particular Toll Service Providers will support the deployment of EFC services on ITS platforms if there is a viable business case present for them. In terms of potential business cases the Toll Service Providers may also benefit from the experiences which they will gain in the context of interoperable regional and EETS services.

It is also expected that once an ITS platform is available in the vehicle (e.g. for purposes of mandatory road safety services) road users will very soon ask for integration of the EFC into that platform.

Toll Chargers may see this development from a different view point. In EFC schemes currently in operation Toll Chargers are used to dedicated EFC hardware and a fairly limited network of (known and trustworthy) Toll Services Providers. This environment will change significantly. Dedicated EFC OBE will disappear and be replaced by in-vehicle platforms that are designed and tested without direct involvement of Toll Chargers. Thus Toll Chargers have less direct influence and control over the hardware platforms in use to operate EFC in their toll domain. Moreover, the number of different hardware platforms will be significantly higher compared to today's EFC OBEs which are available in fairly low number of different versions. EFC as application will share the available resources with other applications of different type and nature. Today's EFC OBE support only EFC as an application. As a general rule one can say that compared to today Toll Charger need to rely more on certification, testing and homologation in a much more complex environment (also comprising more involved actors). Toll Charger will only support such change in case there are precise rules for equipment and service testing and certification as well as for liabilities in place. Such rules shall ensure the expected toll income that shall meet the Toll Chargers performance requirements. Thus Toll Chargers will insist in service level and performance agreements and require methods for monitoring such performance levels.

## 10.2 Actions to reduce barriers for the deployment of EFC applications — Create harmonized certification and test rules

### 10.2.1 Introduction

As laid out at several places in this Technical Report, one of the most important preconditions for EFC on ITS Stations is to provide evidence to the Toll Charger that the EFC service on the ITS Station is trustworthy and reliable to collect the fee according to the expected service level. In most EFC system the equal treatment in relation to the external-cost charge element of a toll (see e.g. 2011/76/EC, Article 7i 2. and Article 7j 2) of all Users, independent of the used devices and processes to pay the fee in a toll domain, is very important. This means that an EFC service running on an ITS Station shall perform on the same service level as a dedicated EFC OBE.

To provide this trustworthiness and ensure the agreed service level of the EFC service on an ITS Station a test- and certification suite shall be established.

### 10.2.2 Issuing test rules

To enable several ITS Station Service Providers with different types of ITS Stations to host the autonomous or DSRC based EFC service in a closed toll domain, the Toll Charger shall issue a standardised suitability for use test procedure and certification procedure. In an interoperable EFC environment with toll domains having different charging rules and charging technologies, the System Management (also called Interoperability Management of the interoperable EFC environment) shall issue this test and certification suite. If the System Management has not the legal power to define a mandatory test and certification suit, the group of all Toll Chargers shall define and agree on such a test suit and certification process.

#### 10.2.3 Guidelines on certification and tests

The certification and test suit for EFC on ITS Stations shall cover two steps.

In a first step the ITS Station shall be certified and tested against a harmonized set of requirements which enables the ITS Station to host an EFC application in the given monolithic or interoperable EFC environment. A first guideline and starting point to define this set of requirements can be found in 7.3. The target of this first step is to ensure that the ITS Station has the required hardware and software resources, i.e. enough computing capacity and all require EFC application interface functions are available. In addition the certification of the required security functions for EFC will be checked.

The second step is a test suite for the verification of the EFC application functionality hosted on the ITS Station. This test suite shall cover all requirements of the suitability for use test and certification procedure (comparable to the description in 9.4) for a harmonized interoperable EFC environment.

The first step of the test and certification procedure described in this subclause should be done only once for an ITS Station and also only once for the second step, the combination of ITS Station and EFC service in an interoperable EFC environment. The successful validation should be accepted by each involved Toll Charger as “suitable for use” in his toll domain.

NOTE 1 The current practise of certification and suitability for use tests as known from the EETS development is clearly indicating that the Toll Chargers will not accept in the short- and mid-term such a single test process as suggested above. But this is indeed required to improve business cases for TSP and drive deployment of EFC on ITS Stations.

NOTE 2 Toll Chargers will require a toll domain dependent certification and suitability for use tests until they are convinced that such a single test process as suggested above is assuring all of their own needs according to the required service level. Currently first interoperable DSRC based EFC systems having agreed on such solution for dedicated EFC OBEs (e.g. EasyGo).

### 10.3 Recommendations for further standardization activities

#### 10.3.1 Recommendations with regard to the area of EFC

##### 10.3.1.1 Role model

The area of EFC is well standardized. The available standards comprise a role model (see ISO 17573) that specifies the tasks and responsibilities of the involved roles and the interfaces between these roles. This role model is well established and accepted and thus forms the ground for the future interoperable EFC services in Europe including the EETS.

However, as outlined in the previous clauses, an amendment to the existing EFC role model seems to be required in order to deploy and operate EFC services in the environment of C-ITS. This amendment should provide a specification for

— additional interfaces and interactions from the EFC role to/with roles that are active in the C-ITS; and

— amendments in the tasks to be carried out by the EFC roles in case EFC services will be made available in the C-ITS environment.

#### 10.3.1.2 Application data definitions

EFC application data are mainly specified in EN ISO 14906 and CEN ISO/TS 17575 (all parts). In addition data for the compliance checking and augmentation communication purposes are made available in standards CEN ISO/TS 12813 and CEN ISO/TS 13141.

The abovementioned standards undergo a periodic and systematic review process carried out by CEN TC 278 WG1. There are no short and mid-term changes expected as a result of deployment of EFC systems on ITS-S. However, in case on a long term horizon the use of EFC at ITS-Ss might lead to approaches and concept in road user charging that completely differ from ideas known and envisaged today a review and potential update of application data definitions may be required.

There is an increasing demand for road users financing the road infrastructure. Ideas about new toll schemes go far beyond the commonly known and widely deployed EFC schemes, that mainly focused on charging HGV traffic for the use of the primary road network and passenger vehicle traffic for the use of high level road network and particular road infrastructure objects like tunnels and bridges. It is expected that electronically supported toll schemes may be expanded towards all levels of road network and all vehicle classes.

In such case EFC data definitions need to provide the ground for such future EFC Tolling Schemes. The data definitions may then require amendments e.g. in the areas of:

— vehicle classification and vehicle characteristics (based on which future toll tariffs may depend);

— toll context description (improved methods of description and supporting the re-use of information available on the in-vehicle ITS-S);

— charge reporting rules (support of future toll schemes);

— compliance checking (future toll schemes may require amended compliance checking data).

#### 10.3.1.3 Compliance checking

A standard is in place which fulfils the needs of today's EFC toll schemes with respect to compliance checking communication. In addition work is on-going to amend the available specification to support method of secure monitoring and trusted recorder.

These currently known methods which support the operational processes of road user compliance checking need to be reviewed and amended once EFC services will be made available via in-vehicle ITS-S. This review and possible update should also take into account the fact that more roles and actors will be involved compared to an EFC only environment. In addition future compliance check / secure monitoring concepts may benefit from better security provisions available as integral part of the in-vehicle ITS-S.

#### 10.3.1.4 EFC security

In case in the future EFC applications will use ITS-S as a basis new security threads may arise (compared to the currently existing situation which is determined by EFC applications on dedicated equipment). First considerations on such threads and potentially required enhancement of EFC security rules and specifications are provided in Annex A of this Technical Report.

#### 10.3.1.5 EFC test standards

In order to ensure compliance to standards and specifications Toll Chargers require harmonized test standards to be used by their suppliers and Service Providers. This demand will increased in case EFC services are made available via C-ITS platforms as more stakeholders, actors and interfaces are involved. Toll Chargers will still insist in a set of standard tests to be carried as part or precondition for certification.

Thus EFC test standards should undergo a review in order to make them compliant to the new requirements and environment in which EFC applications are provided. For details on possible future certification refer also to 10.2.

### 10.3.2 Recommendations with regard to the area of (C-)ITS

For C-ITS both the architecture (see 5.3.1) and the required minimum set of communication media and protocols (see 5.3.2) has been standardized. For the application domain of EFC several standards (EN ISO 14906, EN ISO 12855, CEN ISO/TS 17575 (all parts)) defining the required message sets also exist. But to create benefits from the synergies as described in 9.2 a well-defined and standardised facilities layer is required.

From ETSI/TR 102 638 the facilities layer is separated into three main areas of functionality:

— application support – the kernel of common functions supporting applications, includes lifecycle management, automatic services discovery, download and initialization of new services, HMI generic capabilities, and so on;

— information support (includes presentation layer of the OSI reference model) – manages and provides data, e.g. position, maps, LDM, vehicle characteristics, payment means..;

— communication support (includes session layer of the OSI reference model) – cooperate with the transport and network layer to achieve the various communication modes required by the applications.

For each of these areas a comprehensive set of generic functionality need to be specified. This should be within the scope of CEN TC278 WG16 / ISO TC204 WG18. Based on such standards for generic functionality a mapping to platform specific application programming interfaces (APIs) can be performed. This is illustrated in Figure 25.

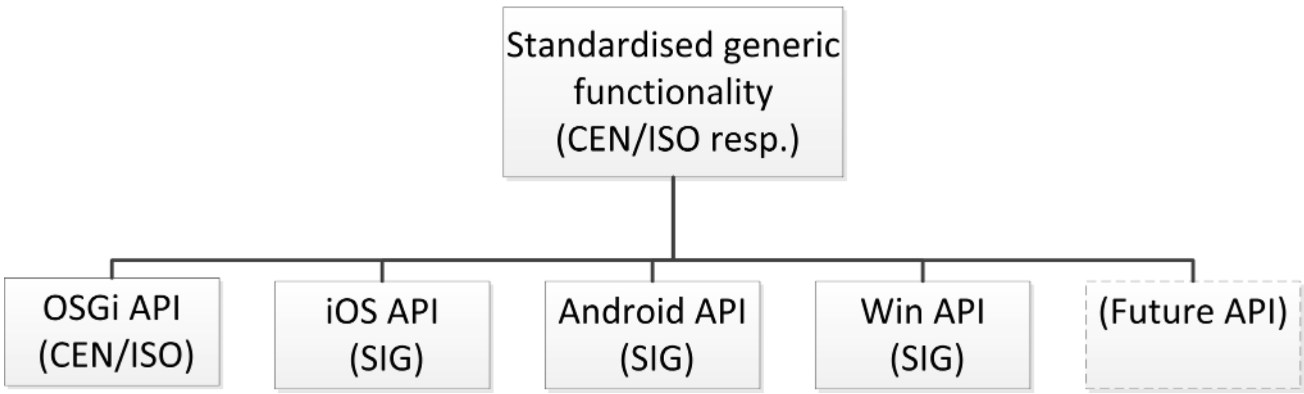



**Figure 25 — Standardising of generic functionality and mapping to APIs**

As stated the work of standardising the generic functionality of the facilities layer should be within ISO/CEN. The required mapping to platform specific APIs might be performed by special interest groups (SIG as shown in the Figure 25). To ensure proper progress and quality of these mapping it might be useful that ISO/CEN also takes the lead to create an API reference implementation. This is exemplified by the OSGi API in Figure 25.

When developing the standards for generic functionality it is important to involve stakeholders from several application domains. This shall ensure a comprehensive facilities layer, but also to have a “jury” ensuring that highly domain specific functionality is kept out. Keeping highly domain specific functionality outside the facilities layer ensures that it is as lean, manageable and bug-free as possible.

To realize future EFC applications on top of in-vehicle ITS-S it is important that stakeholders from the EFC domain participate and cooperate with stakeholders from other domains in defining the generic functionality. This standardization involves identifying and extracting functionality from each domain that can be made generic. From an EFC viewpoint such functionality includes, but is not restricted to, positioning, generic payment services (including micro payment), security, HMI, communication broadcast, application provisioning, application management, application priorities and announcement of mandatory applications.

CEN PT1601 is currently working on two standards for application management in the context of C-ITS, prCEN ISO/TS 17419, *Intelligent transport systems — Co-operative systems — Classification and management of ITS applications in a global context*, and prCEN ISO/TS 17423, *Intelligent transport systems — Co-operative systems — ITS application requirements and objectives for selection of communication profiles*. prCEN ISO/TS 17423 defines communication parameters to be presented by applications to the ITS Station management. These parameters allow the management to grant fair and authorized access of applications to the communication layer in an ITS Station.

## 10.4 Best practice

Many EFC systems are in daily operation in all regions in Europe. Such systems reliably generate millions of toll transactions every day and thus secure the toll revenues for the operators and owners of the road infrastructure. During the design, implementation and operation phases of these EFC systems valuable experiences in various areas have been made.

To benefit from such existing experiences and know-how is seen as key for a successful design and deployment of future EFC services on ITS platforms. Particular best practice which can provide value is e.g. available in the following areas:

a) achieve good results in standardization and thus create acceptance of the standards by:

   1) create and apply a role model in which the tasks, responsibilities and interactions of the involved roles are described;

   2) create a consistent set of interface standards;

   3) reduce and limit complexity by limiting the number of standards and options;

   4) make use of a tool-box approach and create profile standards;

   5) ensure backwards compatibility with existing technology and deployments when updating and revising standards;

b) ensure compatibility with specifications and interoperability amongst systems and devices by:

   1) create test standards which complement the major interface standards;

   2) involve the industry (device and technology manufacturer) in the creation of test standards to make use of their particular experiences;

c) create the ground for a competitive multi-vendor market:

   1) encourage designers of EFC (ITS-) systems and specifications to reuse existing standards,

   2) make interoperability a key requirement in the design of EFC (ITS-) systems;

d) take operational requirements on board at a very early stage in the design of (ITS-)services and roles models;

e) establish harmonized rules for certification and conformity testing.

# Annex A
(informative)

# Security Considerations

## A.1 Introduction

### A.1.1 Security areas and targets

Talking about security of an EFC application on an ITS Station which is a multi-application (or multi service) environment leads to several different discussion areas and targets. These security areas and targets are all important but shall be separated clearly for any kind of technical analysis and solution definition. The main different security areas – as also identified in CEN/TS 16439 are:

— system and application availability and reliability (precondition for data availability);

— data security in terms of confidentiality, integrity, authenticity and non-repudiation;

— user privacy protection.

System and application availability and reliability is in some kind a precondition for data security as also data security is a precondition for privacy protection. Nonetheless, each of these three security topics shall be analysed separately because of its individual policy requirements and targets. The following subclauses define the overall targets of these security areas for an EFC scheme.

### A.1.2 System and application availability and reliability

In an EFC scheme, system and application availability and reliability can be defined as uninterrupted detection of all tolling events including regular transmission of charge data, data exchanges at scheduled moments as well as communication with road side equipment and mobile enforcement units. For this reason an appropriate computing architecture has to be in place on an ITS Station to allow operation of the EFC application with defined availability and performance.

### A.1.3 Data security

The data security of an EFC scheme can be defined as a set of structures and processes that provide or improve the protection of the scheme against fraud. A security system is required to achieve a level of evidential quality of the data collected for road user charging, i.e. to establish the trustworthiness of the road usage data. Trustworthiness of data are essential for correct calculation of the charge due, for compliance checking (i.e. by enforcement officers) and for prosecution (i.e. as evidence in court). But trustworthiness relies also strong on system an application availability and reliability and therefore on complete data availability.

Data security is a topic relevant for any kind of EFC scheme and also for some of the other applications on the ITS platform. However, the more complex an EFC system and the ITS Station are, the less secure it tends to be. In case more security and other mechanisms are required, also more chances for attacks are offered. This means that from a data security point of view, EFC schemes based on a simple approach are preferred to schemes based on complex architecture.

### A.1.4 User privacy protection

In an EFC scheme protecting privacy is important from a user acceptance point of view as well as to fulfil the legal requirements expressed in various data privacy and personal data protection laws and directives. Processing of personal data for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible with clear and unambiguous consent from the data subject's consent, i.e. the user. For this reason, personal data shall only be available to persons and processes which are allowed to use such data.

To achieve the goals of user privacy protection, most of the data security solutions can be used. In addition avoiding the collection of not really used personal data are also a very powerful privacy protection principle.

## A.2 Security scope of this annex

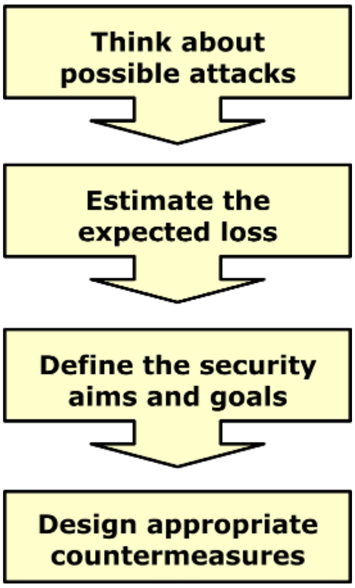
The scope of this annex is mainly data security for EFC schemes as defined in A.1.3. In addition some aspects regarding EFC application availability and reliability will be reflected. These availability and reliability aspects will focus on the problems and solutions on an ITS Station regarding the uninterrupted detection of charge events.

Outside of the scope is any discussion and analysis concerning user privacy protection. This Technical Report relies for ensuring privacy in the context of an ITS Station on the concepts defined by the ETSI standards listed in 5.3.4.

## A.3 General EFC security considerations

### A.3.1 Security analysis

The process for the security analysis of an EFC system is shown in Figure A.1. A threat analysis can be performed to identify security requirements based on existing and latent threats. A detailed thread analysis with regards to EFC is provided in CEN/TS 16439:2013, Annex D The figure below shows the structured process of a threat analysis.




The process starts with searching for and thinking of all possible threats and attacks.

The second step contains a risk assessment. In the risk assessment the expected loss caused by a successful attack is estimated.

The definition of a security policy contains the aims and goals for the security system. The definition process is driven by the insights gained in the risk assessment.

In the last step the appropriate countermeasures, the security architecture and its legal foundation are designed.

**Figure A.1 — Threat analysis**

The first step requires a threat analysis of the whole EFC system, which includes the EFC applications on the several ITS Stations and ITS Station itself. In this first step all kind of threats, including threats concerning availability and reliability of the ITS Station and the EFC application shall be analysed.

The second step contains an estimation of expected reduction income for the TC and TSP, loss of road safety due to non EFC compliant behaviour of drivers and fleet operators. On an ITS Station also the estimation of attacks on an EFC system influencing road safety applications and therefore also results in more danger for road users shall be taken into account. The expected loss is hard to measure and to quantify. To what extent a reduction in road safety caused by a potential attack is acceptable is a policy issue and finally a political decision by the jurisdictions.

The definition of the envisaged security policy in the third step lies in the responsibility of the owner of the toll charging system. The policy shall fulfil all requirements of the charge system legislation. But in case of using ITS Stations, the existing ITS Station architecture and implementation will limit the possible security countermeasures and therefore also possible policy decisions.

In the fourth and last step, the security countermeasures will be defined. In contrast to a complete new designed EFC system, using ITS Stations as the running platform the usable basic security anchors are delivered from the ITS Station. This is the most important limiting factor if a certain required hardware function is not available.

Finally, a security system is not a static solution. This fact is demonstrated to us daily; consider, for example, the alerts released by Microsoft on a near monthly basis. One essential security requirement is therefore the continuing loop of monitoring, analysing and improving the security system.

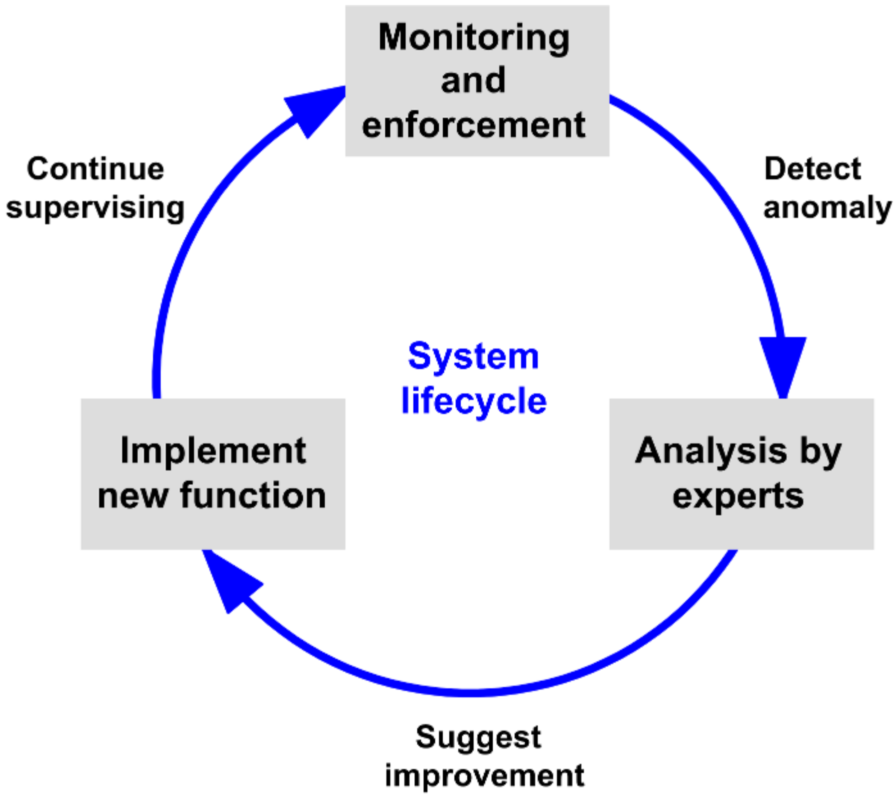



**Figure A.2 — Security system lifecycle**

### A.3.2 Security system

#### A.3.2.1 General

The security system of a EFC scheme shall include countermeasures against threats related to core system assets, such as tamper-proof or tamper-evident data storage and software, and data integrity and authentication mechanisms. In all cases, the security system shall be a closed chain that prevents any manipulation of data and any data “listening”. But it is important that the security system also includes the protected generation of EFC data, which is the uninterrupted detection of all tolling events. Security measures and countermeasures against threads in EFC have been specified in CEN/TS 16439:2013, Clauses 7, 8 and 9.

In general, a distinction can be made between the technical and the organisational architecture of the security system.

#### A.3.2.2 Technical security architecture

The technical architecture of the security system consists of technical components that protect the data from illegal changes, and detect and report attempts of unauthorised manipulation. In general, the transfer of personal data in an EFC scheme should be limited to what is necessary and sufficient to satisfy the conditions based on legal and contractual grounds. Encryption methods and participants authentication should be used to protect all communication processes from access by unauthorised parties.

The ITS Station should support at least tamper evidence – if possible tamper protection - and provide mechanisms for data integrity and authentication. This requires a secure token (e.g. a trusted recorder) inside the ITS Station. Such a secure token stores the private keys and certificates, and prevent them from duplication and falsification. A secure token can also contain cryptographic functions, such as signing and signature verification, encryption and decryption. Secure tokens are copy protected and access restricted storage and cryptographic computing devices, such as the secure chips used in smartcards.

Each ITS Station combined with the EFC application should have a unique identifier (EFC-ID) linked to only one vehicle for the duration of the corresponding account. An EFC application on a ITS Station with redundancy (e.g. using multiple sources to gather distance information) and/or fraud resistance features (e.g. fixed installation in the vehicle) further helps preventing fraud possibilities, and therefore can result in less compliance checking effort.

The backbone of the technical architecture of a security system might be a Public Key Infrastructure (PKI). This infrastructure is based on the widely used public key cryptography, where the key used to encrypt a message is not the same as the key used to decrypt it. The PKI allows protection of a message by creating a digital signature of it using the so-called private key, which can be verified using the so-called public key. It also allows protection of the confidentiality and integrity of a message by encrypting the message using the public key, which can only be decrypted using the private key. The private key is kept secret, whereas the public key may be widely distributed.

#### A.3.2.3 Organisational security architecture

The organisational architecture of the security system has to do with roles, responsibilities and procedures to protect the EFC scheme against fraud and to ensure the required level of data quality.

To reduce the risk of fraud and to prosecute violators, it is important to define the responsibilities of the different actors and the User role. The driver should be legally responsible for checking the operational status of the EFC application (including the ITS Station) before and during each trip on the toll road network and for correctly operating the EFC application, especially with respect to the correct input of the variable vehicle parameters. The vehicle operator as the charge payer should be legally responsible for correct vehicle registration and for payment. In all cases, any form of manipulation of the EFC scheme (e.g. shield the antenna, disconnect the ITS Station from the power supply, develop or possess a tampering device) should be forbidden and prosecuted by law.

In general, the legislation required for road user charging shall provide a basis for a solid security system. This means that:

— The legislation should express a security policy with precise definitions of the required data quality for road user charging.

— The legislation should provide a framework for both technical countermeasures against threats (e.g. digital signatures) and procedural countermeasures against threats (e.g. roadside compliance checking, auditing).

Two main procedural countermeasures against threats are roadside compliance checking and auditing. Fixed and mobile roadside compliance checking can be used to collect evidence about non-compliant Users. Auditing of the haulier's financial and operational bookkeeping may deliver indications of fraudulent behaviour and be a starting point for more detailed on road compliance checking. An additional approach to improve compliance checking which is seen close to auditing might be data mining of all records stored. Although data mining is a sensitive area because of possible privacy infringement, it has the potential to increase evidential data quality by cross-comparing all available (“enforcement archive”) data. Data mining should be conducted by an independent entity with a proper legal foundation.

A certification process for the equipment (e.g. EFC application and ITS Station) and an auditing process for the service providers of the EFC scheme might be useful to guarantee the required level of data quality. This especially applies to EFC service providers who compete on an open market (e.g. EETS) and might benefit from manipulation to make their services more appealing to the User. In case the EFC service provider is mandated (e.g. EFC service provider is a national legal entity), this reduces the security threats, because they do not directly benefit from any kind of manipulation. In all cases, internal cheating (e.g. calculating less tolls for friendly companies) shall be prevented.

Generally, a so-called trusted third party is responsible for security key management. This means that the trusted third party will issue the secure tokens for the EFC application and/or ITS Station and the public key certificates for each User containing data that cannot be forged, such as User identity, public key, validity conditions and possibly other attributes. Besides security key management, trusted third parties can also be used for other services, such as consulting, adjudication and mediation.

## A.4 System and application availability and reliability

As mentioned in the introduction to this annex, system and application availability and reliability are preconditions for data security in terms of application performance and data, i.e. toll event completeness.

The EFC security solution can only with a few limited concepts improve the system availability and reliability but it should if ever possible detect and report unavailability of system resources for the EFC application to the EFC service provider back end.

A main principle to improve availability and reliability is to protect the runtime environment of the EFC service from attacks and failures of other services and applications running on the ITS Stations. This is one method to protect the EFC service on the hosting platform against denial of service attacks. Subclauses 9.5.3.3 and 9.5.3.5 describe two different possible solutions to achieve this goal. But the protection of the communication channel, the protection of the road usage input sensor is not improved against denial of service attacks by this measure.

Such denial of service or other attacks shall be registered by the EFC service and later on, if everything is again operating well, sent to the TSP and TC. The TSP and/or TC shall then take organisational measures to prevent such attacks in future if possible.

## A.5 Security of an ITS Station

### A.5.1 General

It may be assumed that in the future a single ITS Station will provide a variety of ITS applications. Such an ITS Station can host regulatory and commercial applications side by side, using the same central processing unit, memory and other resources (see 9.5.3). The applications may have intended or accidental side effects and impacts on each other. These mutual influences give rise to security concerns.

The main ITS Station application configurations as discussed in 9.5.2 can be defined in two groups:

a) closed ITS Station application platform:

   1) regulatory ITS Station;

   2) closed ITS Station;

b) open ITS Station application platform:

   1) EFC ITS Station;

   2) multi-application ITS Station.

### A.5.2 Closed ITS Station application platform

The security system for a Regulatory ITS Station or a Closed ITS Station is relatively easy to manage, because of the limited application domain. Remaining security risks are low due to the clear and transparent certification or acceptance testing processes for the applications and hardware of both ITS Station types.

**Certification limitations:**

The functionality of an ITS Station and its applications can be validated and certified by a proper test suite. This includes the availability of data in any test case for the tested configuration. But it is important to understand that this does not proof that there is no possible malfunction because no test suite will be able to consider any possible situation of such a complex system.

It is important to understand, that certification has additional limitations when it comes to certification of security. Security as a feature of a system is not testable because you can only test for example the proper encryption or signing function. But this does not give any evidence that the complete implemented security solution is not vulnerable. The security feature of a system shall be verified by a security evaluation process.

The standard ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*, provides a complex guideline for security certification. In this standard the security certification is based on a security evaluation. The evaluation process establishes a level of confidence (Evaluation Assurance Level, from low EAL1 to high EAL7 security) that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs. It is also important to understand that the target of (security) evaluation for example can be the ITS Station, the EFC application or the complete ITS Station including all applications. The more complex a target of evaluation is, the higher the costs for the certification.

NOTE 1 A higher EAL means nothing more, or less, than that the evaluation completed a more stringent set of quality assurance requirements. It is often assumed that a system that achieves a higher EAL will provide its security features more reliably (and the required third-party analysis and testing performed by security experts is reasonable evidence in this direction), but there is little or no published evidence to support that assumption.

NOTE 2 Certification and evaluation of systems like an ITS Station including an EFC application are very seldom because of the huge effort and costs. In fact no existing OBE has been certified above EAL3. State of the art is that smart cards (secure tokens) are evaluated and certified on EAL4 or higher.

### A.5.3 Open ITS Station application platform

The security issues with an open ITS Station application platform are an order of magnitude more complex as a result of its flexibility. This necessitates a flexible security solution that supports many functions. The complexity of such an ITS Station is comparable to a current smart phone or even to a personal computer, which are similar multi-application environments. Such an ITS Station requires a well-designed security system in order to minimize the remaining risks to a level acceptable for a Toll Charger.

EXAMPLE The EFC application may be installed in a Trusted Execution Environment as it is specified by Global Platform (www.globalplatform.org) for an open ITS station to reduce the remaining risks for EFC.

## A.6 Summary

In summary, it can be said that most of the security issues apply not only to EFC applications on an ITS Station. It is therefore recommended to implement from the start a consistent and comprehensive security system on an ITS Station that covers security requirements for all expected applications. Exploiting the available synergies is also essential for a cost-effective future-proof security system. Note that security requirements tend to limit commercial freedom, since security solutions always require some level of regulation, standardization and prescription.

A Toll Charger will accept an ITS Station based EFC solution if he is confident that the reaming risk will not lead to an unacceptable loss of income and all EFC Users are treated equally. It is the task of the security solution for the ITS Station and EFC solution to give the required proof on this issues.

# Bibliography

[1] EN 12253, *Road transport and traffic telematics - Dedicated short-range communication - Physical layer using microwave at 5,8 GHz*

[2] EN 12795, *Road transport and traffic telematics - Dedicated Short Range Communication (DSRC) - DSRC data link layer: medium access and logical link control*

[3] EN 12834, *Road transport and traffic telematics - Dedicated Short Range Communication (DSRC) - DSRC application layer*

[4] CEN/TR 16219, *Electronic Fee Collection - Value added services based on EFC on-board equipment*

[5] CEN/TS 16439:2013, *Electronic fee collection - Security framework*

[6] prCEN ISO/TS 17419, *Intelligent transport systems — Co-operative systems — Classification and management of ITS applications in a global context*

[7] prCEN ISO/TS 17423, *Intelligent transport systems — Co-operative systems — ITS application requirements and objectives for selection of communication profiles*

[8] prCEN ISO/TS 17427, *Intelligent transport systems — Co-operative systems — Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems*

[9] EN ISO/TS 17574, *Electronic fee collection - Guidelines for security protection profiles (ISO/TS 17574)*

[10] ETSI/TS 102 486, *Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment*

[11] ETSI/TR 102 638, *Intelligent Transport Systems (ITS) — Vehicular Communications; Basic Set of Applications; Definitions*

[12] ETSI/TS 102 731, *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*

[13] ETSI/TS 102 792, *Intelligent Transport Systems (ITS) — Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range*

[14] ETSI/TS 102 940, *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*

[15] ETSI/TS 102 941, *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*

[16] ETSI/TS 102 942, *Intelligent Transport Systems (ITS); Security; Access Control*

[17] ETSI/TS 102 943, *Intelligent Transport Systems (ITS); Security; Confidentiality services*

[18] Draft ETSI EN 302 663, Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band

[19] ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture

[20] ISO/IEC 10746 (all parts), Information technology — Open distributed processing

[21] ISO/TR 12859, *Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems*

[22] ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

[23] ISO/DTR 17465 (all parts), Intelligent transport systems — Cooperative ITS

[24] ISO 21210, *Intelligent transport systems — Communications access for land mobiles (CALM) — IPv6 Networking*

[25] ISO 21212, *Intelligent transport systems — Communications access for land mobiles (CALM) — 2G Cellular systems*

[26] ISO 21213, *Intelligent transport systems — Communications access for land mobiles (CALM) — 3G Cellular systems*

[27] ISO 21214, *Intelligent transport systems — Communications access for land mobiles (CALM) — Infra-red systems*

[28] ISO 21215, *Intelligent transport systems — Communications access for land mobiles (CALM) — M5*

[29] ISO 21217:2010, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

[30] ISO 21218, *Intelligent transport systems — Communications access for land mobiles (CALM) — Access technology support*

[31] ISO 24102-4, *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 4: Station-internal management communications*

[32] ISO 24102-5, *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 5: Fast service advertisement protocol (FSAP)*

[33] ISO 29281-1, *Intelligent transport systems — Communication access for land mobiles (CALM) — Non-IP networking — Part 1: Fast networking & transport layer protocol (FNTP)*

[34] CAR 2 CAR Communication Consortium (http://www.car-to-car.org/)

[35] COM(2008) 886, *Action Plan for the Deployment of Intelligent Transport Systems in Europe*

[36] CVIS, D.DEPN.3.1, *Design principles for a privacy protective, secure, safe and fault tolerant CVIS design*

[37] EETS Application guide – Guide for the application of Directive 2004/52/EC of the European Parliament and of the Council and of Commission Decision 2009/750/EC

[38] IEEE 802.11, *IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

[39] IEEE 1609.4, *DSRC multi-channel operations and its implications on vehicle safety communications*

[40] ICT Standardisation Work Program of the European Commission

[41] OVERSEE Project; Open Vehicular Secure Platform (http://www.oversee-project.com)

[42] PLATFORM G. The standard for managing applications on secure chip platform (http://www.openplatform.org)

[43] 85/374/EEC – Council Directive on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

[44] 95/46/EC – Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[45] 2002/58/EC – Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector

[46] 2004/52/EC – Directive of the European Parliament and of the Council on the interoperability of electronic road toll systems in the Community

[47] 2008/671/EC – Commission Decision on the harmonised use of radio spectrum in the 5875-5905 MHz frequency band for safety related applications of Intelligent Transport Systems (ITS)

[48] 2009/750/EC – Commission Decision on the definition of the European Electronic Toll Service and its technical elements

[49] 2010/40/EU – Directive on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport

[50] 2011/76/EU – Directive amending Directive 1999/62/EC on the charging of heavy goods vehicles for the use of certain infrastructures

[51] M/453 – Standardization mandate addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the European Community

*This page deliberately left blank*

# British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

## About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

## Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

## Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

## Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

**PLUS** is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

## Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

## Copyright



## Useful Contacts:

**Customer Services**
**Tel:** +44 845 086 9001
**Email (orders):** orders@bsigroup.com
**Email (enquiries):** cservices@bsigroup.com

**Subscriptions**
**Tel:** +44 845 086 9001
**Email:** subscriptions@bsigroup.com

**Knowledge Centre**
**Tel:** +44 20 8996 7004
**Email:** knowledgecentre@bsigroup.com

**Copyright & Licensing**
**Tel:** +44 20 8996 7070
**Email:** copyright@bsigroup.com

**BSI Group Headquarters**

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™