PD CEN ISO/TS 19299:2015

BSI Standards Publication

Electronic fee collection — Security framework

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This Published Document is the UK implementation of CEN ISO/TS 19299:2015. It supersedes PD CEN/TS 16439:2013 which is withdrawn.

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.

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 87862 6
ICS 03.220.20; 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 October 2015.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 19299:2015

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 19299

October 2015

ICS 35.240.60; 03.220.20

Supersedes CEN/TS 16439:2013

English Version

Electronic fee collection - Security framework (ISO/TS 19299:2015)

Perception de télépéage - Cadre de sécurité (ISO/TS 19299:2015)

Elektronische Gebührenerhebung - Sicherheitsgrundstruktur (ISO/TS 19299:2015)

This Technical Specification (CEN/TS) was approved by CEN on 26 June 2015 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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

© 2015 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN ISO/TS 19299:2015 E

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 19299:2015

Contents

Page

European foreword **3**

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

European foreword

This document (CEN ISO/TS 19299:2015) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Intelligent transport systems” the secretariat of which is held by NEN.

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

This document supersedes CEN/TS 16439:2013.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: 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 the United Kingdom.

Endorsement notice

The text of ISO/TS 19299:2015 has been approved by CEN as CEN ISO/TS 19299:2015 without any modification.

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **2**
3 Terms and definitions ... **4**
4 Symbols and abbreviated terms ... **9**
5 Trust model ... **10**
5.1 Overview ... 10
5.2 Stakeholders trust relations ... 10
5.3 Technical trust model ... 11
5.3.1 General ... 11
5.3.2 Trust model for TC and TSP relations ... 11
5.3.3 Trust model for TSP and service user relations ... 13
5.3.4 Trust model for Interoperability Management relations ... 13
5.4 Implementation ... 13
5.4.1 Setup of trust relations ... 13
5.4.2 Trust relation renewal and revocation ... 14
5.4.3 Issuing and revocation of sub CA and end-entity certificates ... 14
5.4.4 Certificate and certificate revocation list profile and format ... 15
5.4.5 Certificate extensions ... 15
6 Security requirements ... **17**
6.1 General ... 17
6.2 Information security management system ... 18
6.3 Communication interfaces ... 18
6.4 Data storage ... 19
6.5 Toll charger ... 19
6.6 Toll service provider ... 21
6.7 Interoperability Management ... 23
6.8 Limitation of requirements ... 23
7 Security measures — countermeasures ... **24**
7.1 Overview ... 24
7.2 General security measures ... 24
7.3 Communication interfaces security measures ... 25
7.3.1 General ... 25
7.3.2 DSRC-EFC interface ... 26
7.3.3 CCC interface ... 27
7.3.4 LAC interface ... 28
7.3.5 Front End to TSP back end interface ... 28
7.3.6 TC to TSP interface ... 29
7.3.7 ICC interface ... 30
7.4 End-to-end security measures ... 30
7.5 Toll service provider security measures ... 32
7.5.1 Front end security measures ... 32
7.5.2 Back end security measures ... 33
7.6 Toll charger security measures ... 34
7.6.1 RSE security measures ... 34
7.6.2 Back end security measures ... 34
7.6.3 Other TC security measures ... 35
8 Security specifications for interoperable interface implementation ... **35**
8.1 General ... 35
8.1.1 Subject ... 35

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: PD CEN ISO/TS 19299:2015

8.1.2 Signature and hash algorithms ... 35
8.2 Security specifications for DSRC-EFC ... 36
8.2.1 Subject ... 36
8.2.2 OBE ... 36
8.2.3 RSE ... 36

9 Key management ... 36
9.1 Overview ... 36
9.2 Asymmetric keys ... 36
9.2.1 Key exchange between stakeholders ... 36
9.2.2 Key generation and certification ... 37
9.2.3 Protection of keys ... 37
9.2.4 Application ... 37
9.3 Symmetric keys ... 38
9.3.1 General ... 38
9.3.2 Key exchange between stakeholders ... 38
9.3.3 Key lifecycle ... 39
9.3.4 Key storage and protection ... 40
9.3.5 Session keys ... 41

Annex A (normative) **Security profiles ... 42**

Annex B (normative) **Implementation conformance statement (ICS) proforma ... 46**

Annex C (informative) **Stakeholder objectives and generic requirements ... 64**

Annex D (informative) **Threat analysis ... 68**

Annex E (informative) **Security policies ... 124**

Annex F (informative) **Example for an EETS security policy ... 131**

Annex G (informative) **Recommendations for privacy-focused implementation ... 133**

Annex H (informative) **Proposal for end-entity certificates ... 135**

Bibliography ... 136

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/TS 19299 was prepared by European Committee for Standardization (CEN) in collaboration with ISO/TC 204, *Intelligent transport systems*, in accordance with the agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO/TS 19299 cancels and replaces CEN/TS 16439:2013.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Introduction

Reader's guide

The development process for a security concept and implementation to protect any existing electronic fee collection (EFC) system normally includes several steps as follows:

— definition of the security objectives and policy statements in a security policy;

— threat analysis with risk assessment to define the security requirements;

— development of the security measures followed by the development of security test specifications.

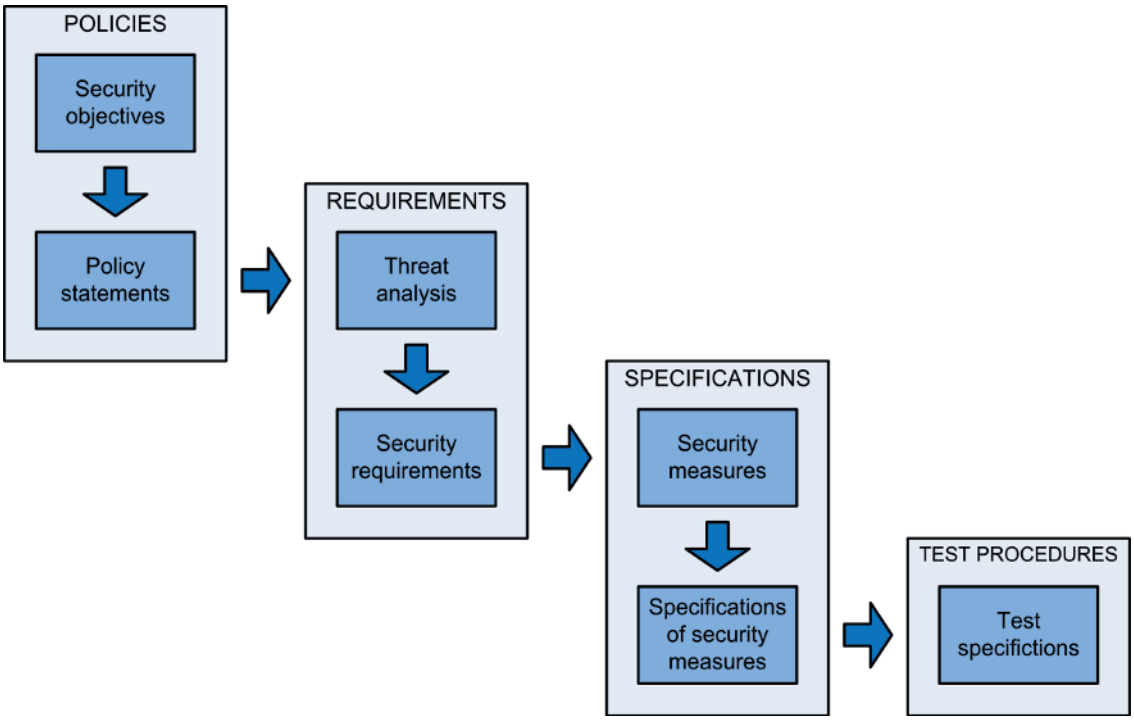

Figure 1 — Development path for the security documents

In the second step, each actor in an existing EFC system has to implement the defined security measures and supervise the effectiveness. Security measures which do not work or work incorrectly need to be improved. The development of the EFC security framework follows this approach as closely as possible. The used methodology needs to consider following limitations:

— No security policy exists: The security policy can only be defined by the responsible stakeholders and its freedom is only limited by laws and regulations. Nonetheless, this Technical Specification provides basic examples of possible security policies (in Annex E to Annex F).

— No risk assessment possible: The risk assessment compares the possible loss for the stakeholder and the required resources (e.g. equipment, knowledge, time, etc.) to perform an attack. It is the trade-off evaluation of the cost and benefit of each countermeasure which is only possible for an implemented system.

— No specific system design or configuration during the development of this Technical Specification was considered to keep it universally applicable. Only the available EFC base standards and the comments received by the CEN/TS 16439:2013 (i.e. the previous edition of the EFC security framework) were taken as references. Specific technical details of a particular system (e.g. servers, computer centres, and de-central elements like road side equipment) need to be taken into consideration during the implementation in addition to the present EFC security framework.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

The selection of requirements and the respective security measures for an existing EFC system is based on the security policy and the risk assessment of several stakeholders systems. Due to the fact that there is neither an overall valid security policy, nor the possibility to provide a useful risk assessment, the EFC security framework provides a toolbox of requirements and security measures covering as many threats as possible without claiming to provide an exhaustive list.

There is one limitation though to be compliant to this Technical Specification that is, if a requirement is selected, the associated security measure(s) have to be implemented.

To understand the content of this Technical Specification, the reader should be aware of the methodological assumptions used to develop it. The security of an (interoperable) EFC scheme depends on the correct implementation and operation of a number of processes, systems, and interfaces. Only a reliable end-to-end security ensures the accurate and trustworthy operation of interacting components of toll charging environments. Therefore, this security framework also covers systems or interfaces which are not EFC specific like back office connections. The application independent security framework for such system parts and interfaces, the Information Security Management System (ISMS), is provided in the ISO 2700x family of standards.

The development process of this Technical Specification is described briefly in the steps below:

a) Definition of the stakeholder objectives and generic requirements as the basic motivation for the security requirements (Annex C). A possible security policy with a set of policy statements is provided in Annex E, and an example of an European electronic toll service (EETS) security policy is given in Annex F.

b) Based on the EFC role model and further definitions from the EFC architecture standard (ISO 17573), the specification defines an abstract EFC system model as the basis for a threat analysis, definition of requirements, and security measures.

c) The threats on the EFC system model and its assets are analysed by two different methods: an attack-based analysis and an asset-based analysis. The first approach considers a number of threat scenarios from the perspective of various attackers. The second approach looks in depth on threats against the various identified assets (tangible and intangible entities). This approach, although producing some redundancy, ensures completeness and coverage of a broader range of risks (see Annex D).

d) The requirements specification (see Clause 6) is based on the threats identified in Annex D. Each requirement is at least motivated by one threat and at least one requirement covers each threat.

e) The definition of security measures (see Clause 7) provides a high-level description of recommended possible methods to cover the developed requirements.

f) The security specifications for interoperable interface implementation (Clause 8) provide detailed definitions, e.g. for message authenticators. These specifications represent an add-on for security to the corresponding relevant interface standards.

g) Basic key management requirements that support the implementation of the interoperable interfaces are described in Clause 9. The toll charging environment uses cryptographic elements (keys, certificates, certificate revocation lists, etc.) to support security services like confidentiality, integrity, authenticity, and non-repudiation. This section of the specification covers the (initial) setup of key exchange between stakeholders and several operational procedures like key renewal, certificate revocation, etc.

h) A general trust model (see Clause 5) is defined to form the basis for the implementation of cryptographic procedures to ensure confidentiality, integrity, and authenticity of exchanged data. In this context, the security framework references approved international standards for the implementation of cryptographic procedures enhanced by EFC specific details where needed.

A stakeholder of an EFC scheme who wants to use this security framework needs to do the following:

— define a security policy for the EFC scheme (may involve more than one stakeholder in an interoperable EFC scheme). Some examples for a security policy and its elements are provided (in

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: PD CEN ISO/TS 19299:2015

Annex E and Annex F) as an aid for using this Technical Specification to build up a secure system for a concrete interoperability framework (including the European electronic toll service).

— identify the relevant processes, systems and interfaces, and match them to the EFC security framework;

— select the corresponding security requirements according to the security policy;

— implement the security measures associated to the selected requirements;

— provide evidence of compliance of its systems, processes, and interfaces with the requirements set forth in this Technical Specification. Evidence can be provided by a self-declaration, an internal or external audit, or other certifications.

EFC role model

This Technical Specification complies with the role model defined in ISO 17573. According to this role model, the toll charger (TC) is the provider of the tolled infrastructure or transport service and hence, the recipient of the road usage fees. The TC is the actor associated with the toll charging role (see Figure 2).

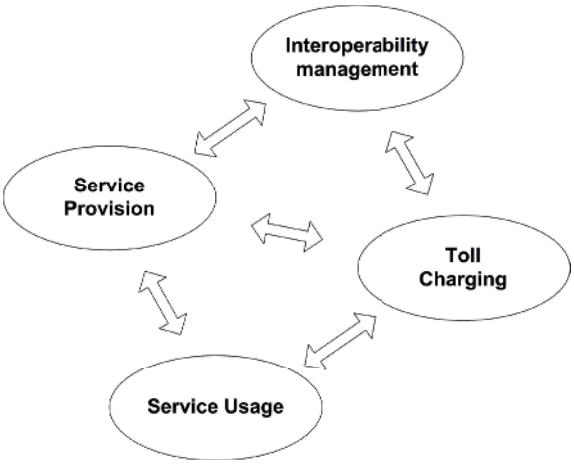

Figure 2 — The role model underlying this Technical Specification

Toll service providers (TSP) issue on-board equipment (OBE) to the users of the tolled infrastructure or transport service. TSPs are responsible for providing the OBE that will be used for collecting data, enabling the TC to send a claim to the TSP for the use of the infrastructure or transport service by their service users (SU). In autonomous systems, each TSP delivers toll declarations to the TC who operates the autonomous system. Such a TC possibly receives toll declarations from more than one TSP. In dedicated short-range communication (DSRC)-based systems, the TC receives the main toll declarations from its own RSE which communicates with the TSP's OBE and only supplementary charging data, if required, from the TSP. Interoperability management (IM) in Figure 2 comprises all specifications and activities that in common, define and maintain a set of rules that govern the overall toll charging environment.

The trust model defined in this Technical Specification is based on the role model above and it is also the technical base for the protection of the data communication between the entities of the role model. Besides this communication security, trust in the secure implementation and management of the back end and other equipment for the EFC framework is required. A toll charger or toll service provider compliant to this Technical Specification needs to be able to give evidence of security management as required. Such evidence is the basis of trust relations between the involved entities.

Figure 3 below illustrates the abstract EFC system model used to analyse the threats, define the security requirements and associated security measures for this Technical Specification. This Technical Specification is based on the assumption of an OBE which is dedicated to EFC purposes only and neither considers value added services based on EFC OBE, nor more generic OBE platforms (also called in-vehicle ITS Stations) used to host the EFC application. The OBE may either be connected to a central

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

account or use a payment medium such as ICC or mobile payment for on-board-account EFC system. Any financial transactions to the payment medium are out of scope of this Technical Specification.

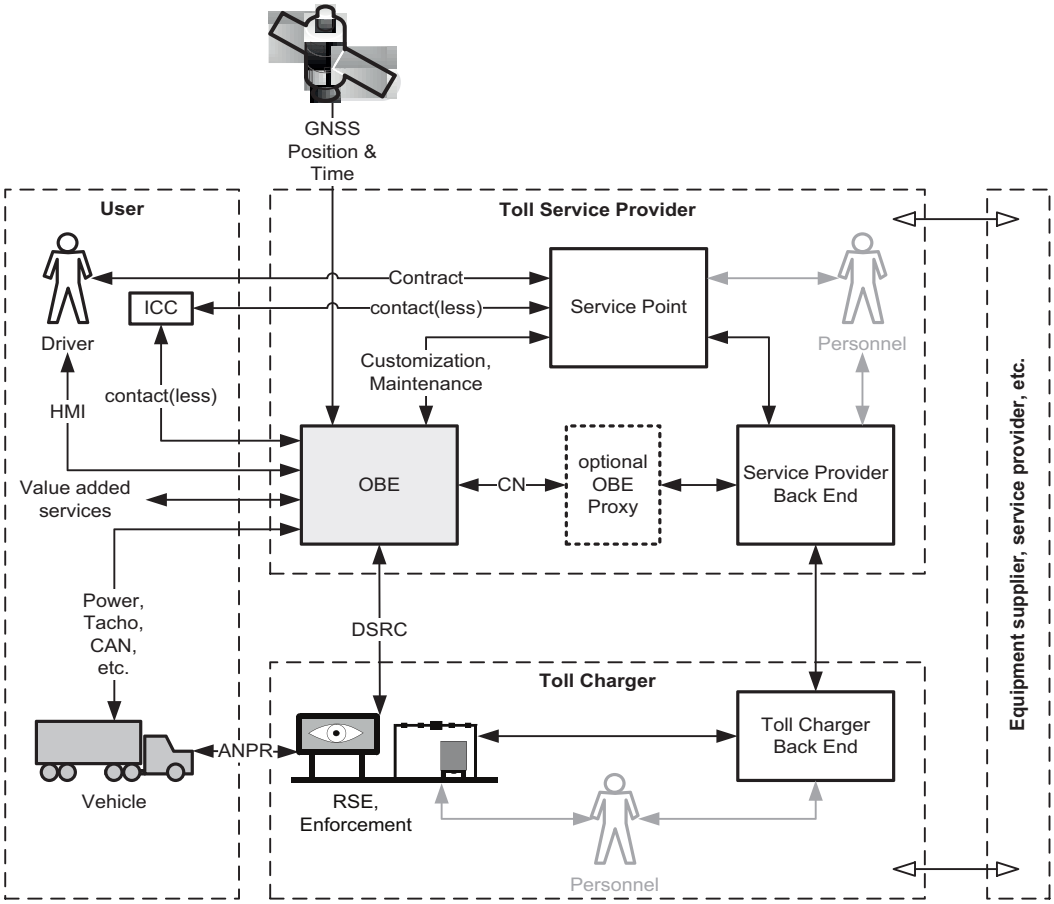

Figure 3 — EFC system model of the EFC Security framework

Relation to other security standards

Several generic and specific standards and Technical Reports concerning security issues for information technology already exist. This Technical Specification uses these existing standards and expands their usability for EFC applications. The framework references and tailors the security techniques and methodologies from these standards.

Figure 4 illustrates the context of the EFC security framework to other security standards. It is not an exhaustive description as only the most relevant standards are shown, i.e. the standards that gave most input to this Technical Specification. Standards that are directly used and referenced are highlighted in black (as opposed to grey). Other standards that may provide other security related input are given for information and completeness only, but are not further used.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

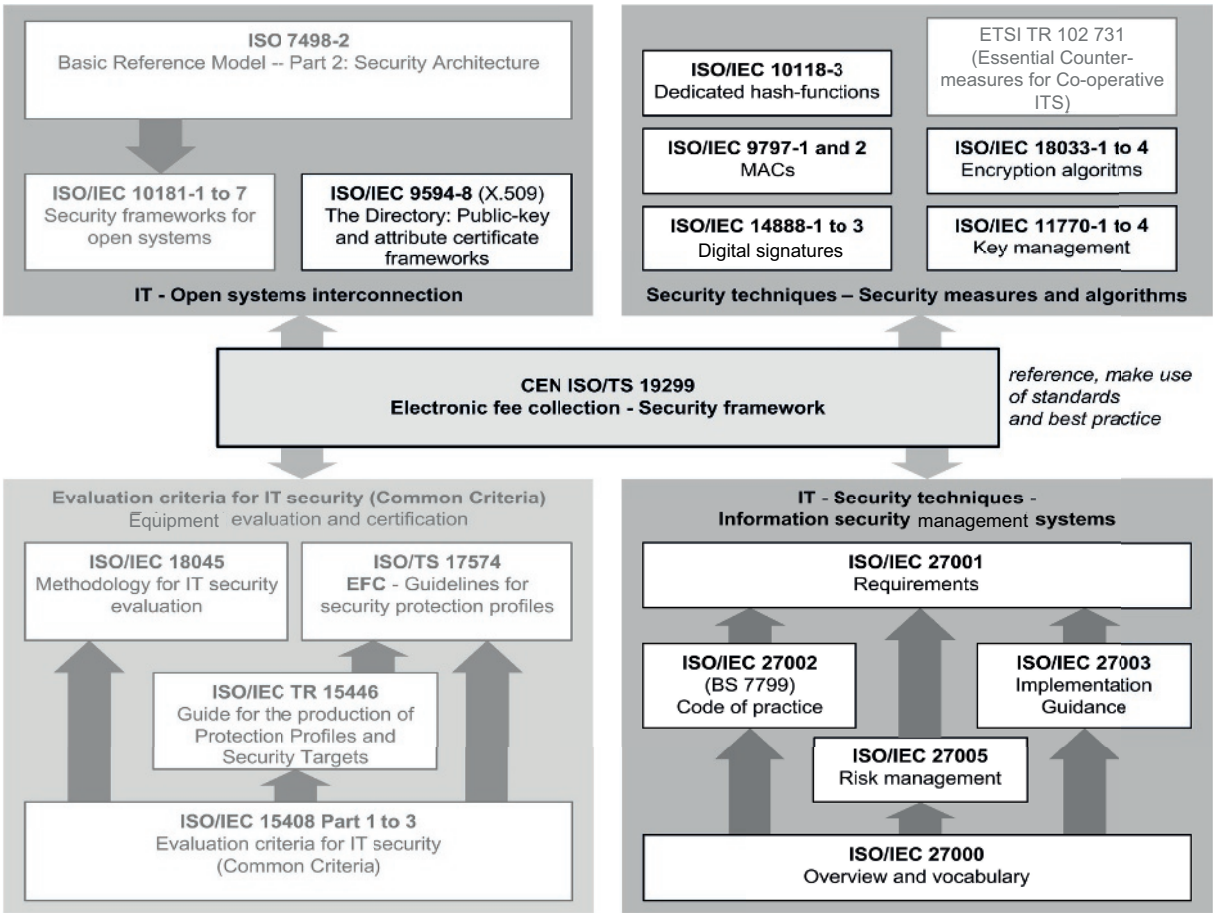

Figure 4 — Relevant security standards in the context of the EFC — Security framework

Each group of standards in Figure 4 provides the following features:

— **Security techniques — Security measures and algorithms**: The group is a collection of essential security measures and recommended cryptographic algorithms including the guidelines for accurate use.

— **IT — Open system interconnection**: This group of standards provides mechanisms for the secure communications between open systems. The standards address some of the security requirements in the areas of authentication and other security services through the provision of a set of frameworks.

— **Evaluation criteria for IT security (common criteria)**: This standard group defines methodologies and processes for the security evaluation and certification for most categories of products used in the EFC environment. The arrows inside the group indicate the relation between the standards in a bottom-up direction.

— **IT — Security techniques — Information security management system**: This standard family defines requirements and guidelines for the implementation of security management systems for all types of organizations. The standards are well suited for the security solutions of the back end and other fixed or installed equipment including software of EFC systems.

A corresponding ISO/IEC 27001 certification of a toll charger (TC) or toll service provider (TSP) organization may be used to demonstrate fulfilment of this Technical Specification provided that the scope and the Statements of Applicability (SoA) include the EFC business processes specified in ISO 17573 and the selected security requirements and their associated security measures provided by this Technical Specification are applied, e.g. by using them as part of the so-called catalogues containing the security measures and control objectives. Figure 5 below illustrates how this approach works in parallel. The first step of both paths is analysing the business processes followed by a threat analysis.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

A common risk analysis combines the generic and the EFC related analysis and results in the respective security measures and controls.

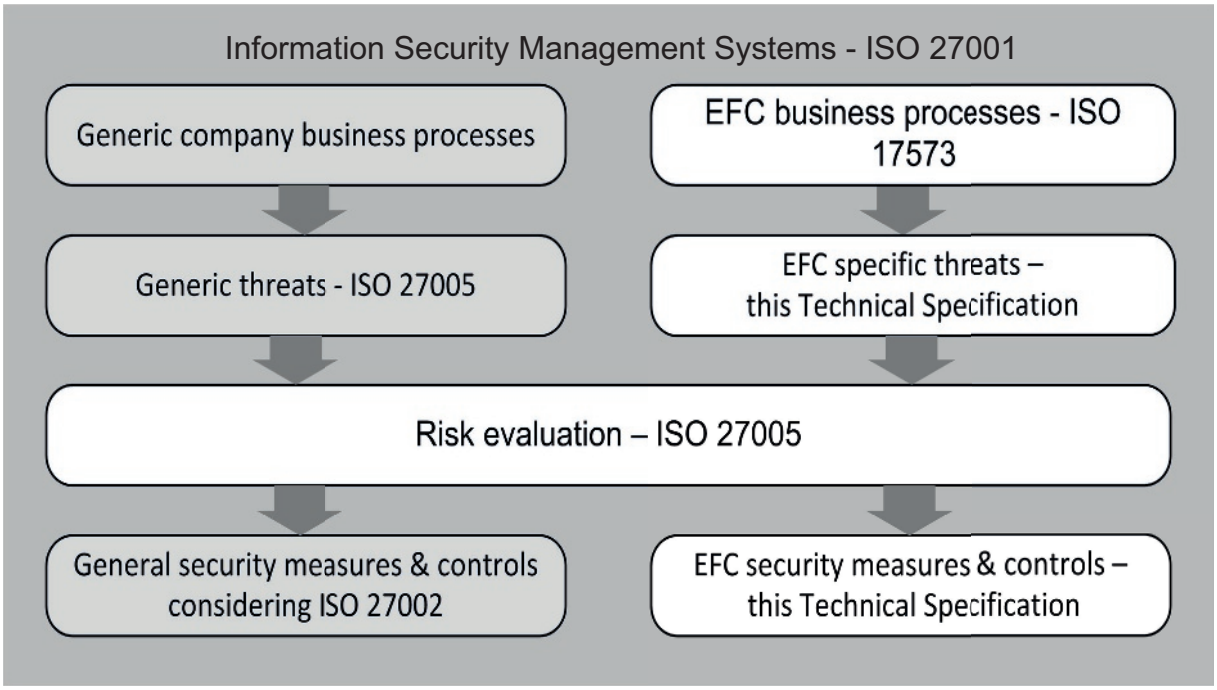

Figure 5 — Scope in relation to the Information Security Management System

In addition, the EFC security framework makes use of existing threat analysis methods and also uses existing threat analysis with relation to EFC or ITS [e.g. ETSI/TR 102 893 (intelligent transport systems; security; threat, vulnerability and risk analysis)].

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Electronic fee collection — Security framework

1 Scope

The overall scope of this Technical Specification is an information security framework for all organizational and technical entities of an EFC scheme and in detail for the interfaces between them, based on the system architecture defined in ISO 17573. The security framework describes a set of requirements and associated security measures for stakeholders to implement and thus ensure a secure operation of their part of an EFC system as required for a trustworthy environment according to its security policy.

The scope of this Technical Specification comprises the following:

— definition of a trust model (Clause 5);

  Basic assumptions and principles for establishing trust between the stakeholders.

— security requirements (Clause 6);

— security measures — countermeasures (Clause 7);

  Security requirements to support actual EFC system implementations.

— security specifications for interface implementation (Clause 8);

  These specifications represent an add-on for security to the corresponding standards. Figure 5 above shows the relevant interfaces and the corresponding relevant interface standards, as illustrated in Figure 6.

— key management (Clause 9);

  Covering the (initial) setup of key exchange between stakeholders and several operational procedures like key renewal, certificate revocation, etc.

— security profiles (Annex A);

— implementation conformance statement (Annex B) provides a checklist to be used by an equipment supplier, a system implementation, or an actor of a role declaring his conformity to this Technical Specification;

— general information security objectives of the stakeholders (Annex C) which provide a basic motivation for the security requirements;

— threat analysis (Annex D) on the EFC system model and its assets using two different complementary methods, an attack-based analysis, and an asset-based analysis;

— security policy examples (Annex E and Annex F);

— recommendations for privacy-focused implementation (Annex G);

— proposal for end-entity certificates (Annex H).

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 19299:2015

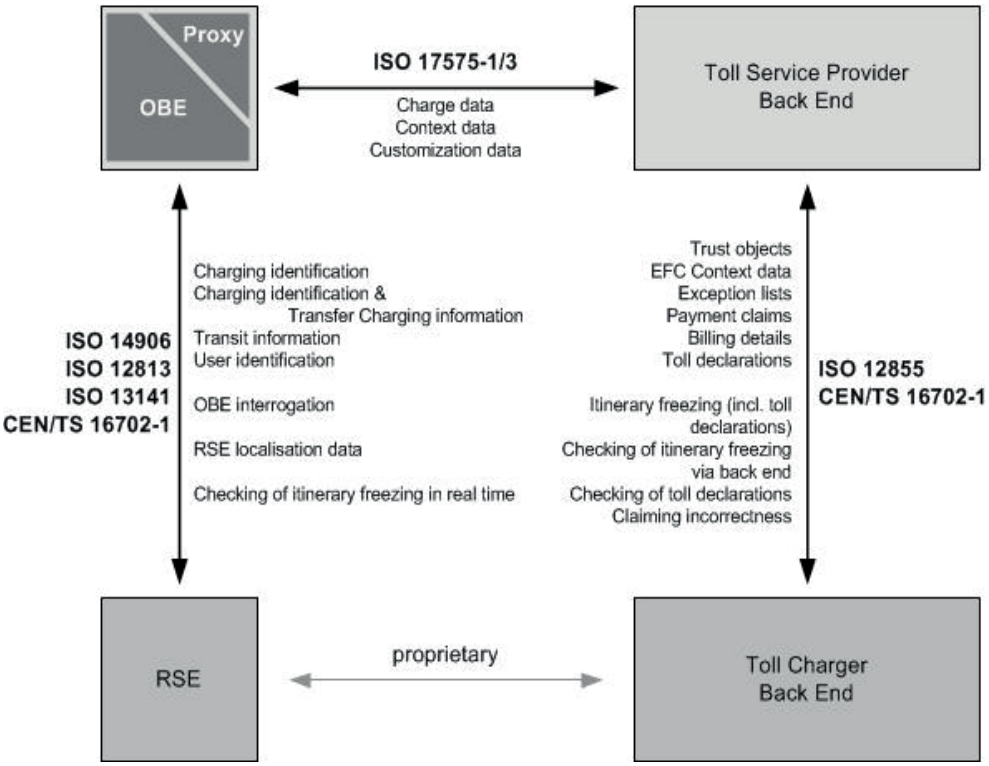

Figure 6 — Scope of EFC security framework for secure communication

The following are outside the scope of this Technical Specification:

— a complete risk assessment for an EFC system;

— security issues rising from an EFC application running on an ITS station;

NOTE Security issues associated with an EFC application running on an ITS station are covered in CEN/TR 16690.

— entities and interfaces of the interoperability management role;

— the technical trust relation between TSP and service user;

— concrete implementation specifications for implementation of security for EFC system [e.g. European electronic toll service (EETS)];

— detailed specifications required for privacy-friendly EFC implementations;

— any financial transactions between the payment service provider and the payment medium issued by the latter (e.g. ICC).

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.

ISO 12813:2015, *Electronic fee collection — Compliance check communication for autonomous systems*

ISO 12855:2015, *Electronic fee collection — Information exchange between service provision and toll charging*

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

ISO 13141:2015, *Electronic fee collection — Localization augmentation communication for autonomous systems*

ISO 14906:2011, *Electronic fee collection — Application interface definition for dedicated short-range communication*

EN 15509:2014, *Electronic fee collection — Interoperability application profile for DSRC*

CEN/TS 16702-1:2014, *Electronic fee collection — Secure monitoring for autonomous toll systems — Part 1: Compliance checking*

ISO 17575-1:2015, *Electronic fee collection — Application interface definition for autonomous systems — Part 1: Charging*

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO/IEC 9594-8:2014, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 11770-1:2010, *Information technology — Security techniques — Key management — Part 1: Framework*

ISO/IEC 11770-3:2015, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

IETF Request for Comments (RFC) 4301:2005-12, *Security Architecture for the Internet Protocol*

IETF Request for Comments (RFC) 4347:2006-04, *Datagram Transport Layer Security*

IETF Request for Comments (RFC) 4648:2006-10, *The Base16, Base32, and Base64 Data Encodings*

IETF Request for Comments (RFC) 5035:2007-08, *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*

IETF Request for Comments (RFC) 5246:2008-08, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF Request for Comments (RFC) 5280:2008-05, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

IETF Request for Comments (RFC) 5746:2010-02, *Transport Layer Security (TLS) Renegotiation Indication Extension*

Federal Information Processing Standards (FIPS) PUB 140-2, December 2002, *Security requirements for cryptographic modules*

3 Terms and definitions

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

3.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[SOURCE: ISO 7498-2:1989, 3.3.3]

3.2
activist
especially active, vigorous advocate of a cause, especially a political cause

3.3
asset
anything that has value to a stakeholder

Note 1 to entry: An asset may be tangible or intangible.

3.4
attack
attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an *asset* (3.3)

[SOURCE: ISO/IEC 27000:2014, 2.3]

3.5
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2014, 2.8]

3.6
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989, 3.3.11]

3.7
back end
part of the back office system interfacing to one or more *front ends* (3.17)

3.8
certificate revocation list
signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

[SOURCE: ISO/IEC 9594-8:2014, 3.5.12]

3.9
key certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

[SOURCE: ISO 15782-1:2009, 3.15]

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

3.10
communication provider
provider of communication services used for the transmission of information

3.11
confidentiality
prevention of information leakage to non-authenticated individuals, parties, and/or processes

[SOURCE: ISO/TS 17574:2009, 3.7]

3.12
data protection commissioner
data privacy commissioner
person responsible for the enforcement and monitoring of compliance with the applicable data protection legislation

3.13
data subject's consent
any freely given specific and informed written indication of his wishes by which the data subject signifies his agreement to *personal data* (3.30) relating to him being processed

3.14
electronic money
value having its equivalence in real money, electronically stored e.g. on a bank account or an IC-card, which thus can be used by the user for payments

[SOURCE: ISO/TR 19639:—, 3.5]

3.15
enforcement
measures or actions performed to achieve compliance with laws, regulations, or rules

Note 1 to entry: In this context, the process of compelling observance of a *toll regime* (3.46).

3.16
foreign state agency
any agency of any state except the state under whose jurisdiction a particular *toll scheme* (3.47) is operated

3.17
front end
part of a tolling system consisting of OBE and possibly, a proxy where tolling information and usage data are collected and processed for delivery to the *back end* (3.7)

3.18
domestic state agency
government or any agency of the state or nation under whose jurisdiction a particular toll schema is being operated

3.19
hacker
person who attempts or succeeds to gain unauthorized access to protected resources

3.20
information asset
knowledge or data that has value to the stakeholder

[SOURCE: ISO/IEC 27032:2012, 4.27, modified]

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

3.21
information security
preservation of *confidentiality* (3.11), *integrity* (3.24), *availability* (3.6), *authenticity* (3.5), *accountability* (3.1), *non-repudiation* (3.27), and reliability of information

[SOURCE: ISO/IEC 27000:2014, 2.33, modified]

3.22
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

[SOURCE: ISO/IEC 27000:2014, 2.35]

3.23
information security incident
unwanted *information security* (3.21) events that have a significant probability of compromising business operations and threatening information security

[SOURCE: ISO/IEC 27000:2014, 2.36, modified]

3.24
integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/TS 17574:2009, 3.11, modified]

3.25
interoperability
ability of systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/IEC/TR 10000-1:1998, 3.2.1, modified]

3.26
message authentication code
MAC
string of bits which is the output of a MAC algorithm

Note 1 to entry: A MAC is sometimes called a cryptographic check value (see, for example, ISO 7498-2).

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

3.27
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: ISO/IEC 27000:2014, 2.55]

3.28
on-board equipment
OBE
equipment located on-board a vehicle including nomadic devices with the function of exchanging information with external systems

3.29
payment medium
carrier of payment means, such as paper ticket, IC-card, smart phone or on-board unit (OBU)

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

3.30
personal data
information relating to an identified or identifiable natural person

Note 1 to entry: In relation to EFC, an identified or identifiable natural person is equivalent to the role service user (ISO 17573:2010).

3.31
policy
overall intention and direction as formally expressed by management

[SOURCE: ISO/IEC 27000:2014, 2.60, modified]

3.32
data privacy
rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/TS 14441:2013, 3.26]

3.33
processing of personal data
operation or set of operations which is performed upon *personal data* (3.30), whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction

3.34
roadside equipment
RSE
equipment located along the road ether fixed or mobile

3.35
secure application module
SAM
physical module that securely executes cryptographic functions and stores keys

3.36
security policy
set of rules that regulate how to handle security threats or define the appropriate security level

[SOURCE: ISO/TS 17574:2009, 3.23]

3.37
security service
service provided by communicating systems which ensures adequate security of the systems or of data transfers

[SOURCE: ISO 7498-2:1989, 3.3.51, modified]

3.38
digital signature
one or more data elements resulting from the digital signature process

3.39
threat
potential cause of an unwanted information security incident, which may result in harm

[SOURCE: ISO/IEC 27000:2014, 2.83, modified]

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

3.40
threat agent
entity that has the intention to act adversely on an *asset* (3.3)

3.41
threat analysis
systematic detection, identification, and evaluation of *threats* (3.39)

3.42
toll
any charge, tax, or duty levied in relation with using a vehicle in a *toll domain* (3.45)

[SOURCE: CEN/TR 16092:2011, 3.6, modified]

3.43
toll charger
TC
entity which levies *toll* (3.42) for the use of vehicles in a *toll domain* (3.45)

[SOURCE: ISO 17573:2010, 3.16, modified]

3.44
toll declaration
statement to declare the usage of a given toll service to a *toll charger* (3.43)

[SOURCE: ISO 17573:2010, 3.17, modified]

3.45
toll domain
area or a part of a road network where a certain *toll regime* (3.46) is applied

[SOURCE: ISO 17573:2010, 3.18, modified]

3.46
toll regime
set of rules, including enforcement rules, governing the collection of *toll* (3.42) in a *toll domain* (3.45)

[SOURCE: ISO 17573:2010, 3.20]

3.47
toll scheme
organizational view of a *toll regime* (3.46) including the actors and their relationships

[SOURCE: ISO/TS 17575-3:2011, 3.35, modified]

3.48
toll service provider
TSP
entity providing toll services in one or more *toll domains* (3.45)

[SOURCE: ISO 17573:2010, 3.23, modified]

3.49
trusted third party
TTP
security authority or its agent trusted by other entities with respect to security-related activities

[SOURCE: ISO/IEC 10181-1:1996, 3.3.30 modified]

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

3.50
service user
SU
generic term used for the customer of a *toll service provider* (3.48), one liable for *toll* (3.42), the owner of the vehicle, a fleet operator, a driver, etc. depending on the context

[SOURCE: ISO 17573:2010, 3.29, modified]

3.51
vulnerability
weakness of an *asset* (3.3) or control that can be exploited by an attacker

[SOURCE: ISO/IEC 27000:2014, 2.89, modified]

4 Symbols and abbreviated terms

AC_CR	Access Credentials (EN 15509:2014)
ADU	Application Data Unit
CA	Certification Authority (ISO 15782-1:2009)
CCC	Compliance Check Communication (ISO 12813:2015)
CN	Cellular Network
CRL	Certificate Revocation List
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication (ISO 14906:2011)
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection (ISO 17573:2010)
GNSS	Global Navigation and Satellite System (ISO 17573:2010)
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over Secure socket layer
ICC	Integrated Chip Card (IC card)
ICS	Implementation Conformance Statement (ISO/TS 14907-2:2011)
IETF	Internet Engineering Task Force
IM	Interoperability Management
IPsec	Internet Protocol Security
ISMS	Information Security management system (ISO/IEC 27000:2014)
LAC	Localization Augmentation Communication (ISO 13141:2015)
MAC	Message Authentication Code
MAC_TC	DSRC Message Authentication Code for toll charger
MAC_TSP	DSRC Message Authentication Code for toll service provider

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

OBE	On-Board Equipment (ISO 14906:2011)
OID	Object Identifier
PAN	Personal Account Number
PER	Packed Encoding Rules (ISO/IEC 8825-2)
PKI	Public Key Infrastructure
RQ	Requirement
RSA	Rivest, Shamir and Adleman

NOTE RSA is an algorithm for public-key cryptography also referred to as asymmetrical cryptographic technique.

RSE	Roadside Equipment (ISO 14906:2011)
SAM	Secure application module
SHA-1	Secure hash algorithm (ISO/IEC 10118-3)
SM	Security Measure (countermeasure)
SU	Service User
TC	Toll Charger (ISO 17573:2010)
TLS	Transport Layer Security
TSP	Toll Service Provider
TTP	Trusted Third Party
VPN	Virtual Private Network
XER	XML Encoding Rules (ISO/IEC 8825-4)

5 Trust model

5.1 Overview

The trust model provides the basic trust and functionality for the implementation of authenticated and secured communication channels between TSP and TC.

The trust model has two different levels, the contractual framework between the stakeholders (TC, TSP, and SU) and the technical trust model between the IT infrastructure of the TC and TSP.

The trust model is based on the assumption that no initial technical trust relation between any of the stakeholders exists or will be generated by a predefined third party.

5.2 Stakeholders trust relations

Three kinds of bidirectional contract-based peer-to-peer trust relations are present in the underlying EFC role model. The following are the peer-to-peer trust relations:

— between toll charger and toll service provider;

— between toll service provider and service user;

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

— between toll charger or toll service provider and interoperability management.

There is no direct trust relation between toll charger and service user, as illustrated in Figure 7. The obligation of the service user is to pay for the transport service (e.g. road use) according to laws and regulations of the respective toll domain by using the OBE issued by the TSP.

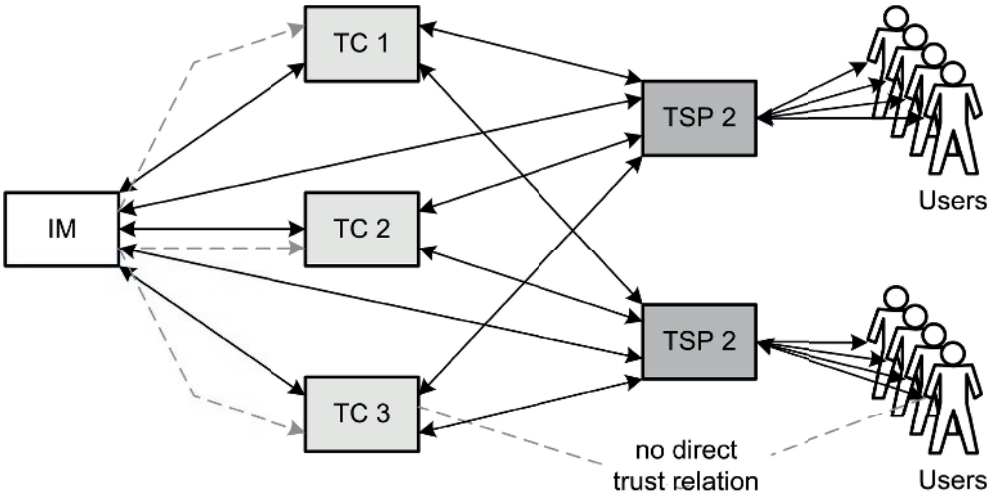

Figure 7 — Stakeholder trust relations

The interoperability management can be a single organization or a construct of several entities performing different tasks. Issuing rules, regulations, and general user information by the interoperability management (IM) is done using a trust relation outside of the scope of this Technical Specification (dotted arrows in Figure 7). Trust relations between IM and TC or TSP inside the scope are among others used for certification of organization or equipment and TTP functions in case this is performed by the IM.

One supported model is an agreement between TC and TSP to use a Trusted Third Party (TTP) (e.g. for issuing public-key root certificates). Such a hierarchical trust relation supported by a TTP can include the IM relations to TC and TSP. The TTP could either be performed as a part of the IM or external TTP(s) could be used to issue the root certificates. This Technical Specification does not require a mandatory TTP in a hierarchical trust model, but supports the use of it.

Another supported model is an agreement between TC and TSP to directly trust them by exchanging self-signed root certificates. Such a peer-to-peer trust relation can also include the IM relations to TC and TSP. This Technical Specification does not require a mandatory peer-to-peer trust model, but supports the use of it.

The technical trust relation of any chosen trust model between TSP and service user (SU) as well as the indirect trust relation between TC and SU are outside the scope of this Technical Specification.

5.3 Technical trust model

5.3.1 General

The technical trust model defines a solution for the trust relations between the different stakeholders. The technical trust model is dependent on the requirements of the concerned stakeholders with respect to support an interoperable EFC system.

5.3.2 Trust model for TC and TSP relations

The technical trust model uses the ISO/IEC 9594-8, (X.509) version 3 public-key and attribute certificate frameworks for establishing secure communication channels. These secure communication channels

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

ensure confidentiality, integrity, authenticity, and non-repudiation (only with proof of origin) of the messages exchanged between TC and TSP.

The use of ISO/IEC 9594-8, i.e. using the possibility to import and use in parallel different (self-signed) root certificates in the trust model, enables the support of both a peer-to-peer approach and a hierarchical approach using a trusted third party. In addition, it also allows a mixed approach with peer-to-peer relations between TC and TSP on one hand and a TTP certification authority (CA) approach on the other hand.

EXAMPLE Figure 8 illustrates an example of a trust model approach which is supported by this Technical Specification.

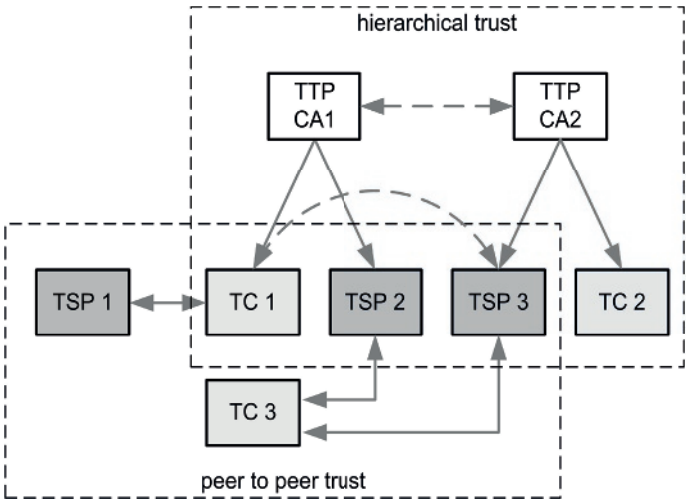

Figure 8 — Example of a mixed trust model environment

Figure 8 indicates the possibility of the trust model allowing an entity to participate at the same time in a mixed environment with both approaches. The dotted box marked as "hierarchical trust" shows the trusted third parties in their roles as certification authorities (CA1 and CA2) issuing certificates for each entity based on its self-signed root certificate imported by the entities. It is also possible that the TTP CAs directly issue certificates for the technical entities communicating with each other. In this case, no root certificate would exist and securing all interfaces would be established by bilaterally accepting self-signed certificates.

A trust relation can also be established across different TTP CAs as indicated by the dotted connections TC1 trusts TTP CA1 and TSP3 trusts TTP CA2. TTP CA1 also trusts TTP CA2 and vice versa. Thererefore, there is also a trust relation between TC1 and TSP3.

The dotted box "peer-to-peer trust" shows entities generating self-signed root certificates for exchange and import of these certificates. Entities in the overlapping part of the boxes (i.e. TC1, TSP2, and TSP3) import both the certificates issued by the TTP CAs and the connected peer-to-peer trust partner (i.e. TC3, TSP1) self-signed root certificates.

The use of the ISO/IEC 9594-8 framework and certificates also enables hierarchical CA structures with a root CA and subordinate level CAs. To limit implementation complexity and to support interoperability, the set of allowed certification levels shall be limited as indicated in 5.4.3.

The used type and structure of the model for the trust relation between the involved stakeholders is a decision of their contractual framework and depends on their technical requirements as well as the legal framework. The IM in an interoperable EFC system shall develop and maintain a suitable trust model. An example for EETS can be found in Annex F.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

5.3.3 Trust model for TSP and service user relations

A standardized trust relation mechanism for the trust between TSP and service user is not required for interoperability. The solution for a trusted and secured communication between TSP and service user is a decision taken by the TSP based on the legal requirements for the contract between TSP and service user.

According to ISO 17573, the operation of the OBE and the provision of toll declarations in a secure way as required for toll charging is part of the toll service provider role. Requirements for achieving end-to-end security from the OBE to the toll chargers systems is therefore considered to be an internal interface of the TSP and then between TSP and TC. If security requirements for end-to-end security are imposed by the security policy, appropriate measures need to be implemented (e.g. usage of CEN/TS 16702-1 or CEN/TS 16702-2).

5.3.4 Trust model for Interoperability Management relations

The interoperability management may issue rules, regulations, and standards for the EFC system via commonly recognized channels. Communication between IM and TC or TSP (e.g. for certification of organizations or equipment) can be done with legacy methods such as physical mail and face to face meetings. No technical trust model is required for either of these communications.

For all other cases where electronic data exchange channels are required, the same technical trust model as defined in 5.3.2 shall be used.

5.4 Implementation

5.4.1 Setup of trust relations

After TC and TSP have agreed on the trust relation to be used and have signed a contract, they shall setup the technical trust relation.

The initial step for the setup of the trust relation is the import of a root certificate. This can be either the CA root certificate of an agreed TTP acting as a root CA or a (self-signed) root certificate of the TC or TSP respectively as already explained in 5.3.2.

If using a TTP, the retrieval of the CA root certificate shall be done according to mechanism 3 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent. Several procedures might be used such as the following:

— downloading the certificate from a recognized and secure website;

— retrieving it per courier, if supported by the TTP;

— receiving it through signed e-mail, etc.

In the case of a peer-to-peer trust model, the exchange of the CA root certificates between TC and TSP shall be done using a secure communication channel which ensures the authenticity of the issuer and sender (proof of origin). The exchange of the root certificates shall be done with one of the public key transport mechanisms 1 or 2 as defined in ISO/IEC 11770-3:2015, Clause 12 (Public key transport).

— Mechanism 1: This mechanism shall fulfil the requirements and implement the measures of mechanism 1 of ISO/IEC 11770-3:2015, Clause 12, but using a certificate instead of a public key. As an example, it may be implemented by a physical meeting when both stakeholders (representatives of the TC and TSP, respectively) exchange valid identification tokens (e.g. passport) and documents proving the relationship with their organization.

  ISO/IEC 11770-3 public key transport mechanism 1 may be implemented as a part of the contract signing process to guarantee the certificate and public key authenticity.

— Mechanism 2: This mechanism shall fulfil the requirements and implement the measures of mechanism 2 of ISO/IEC 11770-3:2015, Clause 12, but using a certificate instead of a public key. As an example, it may be implemented by sending the root certificate through signed e-mail (using

© ISO 2015 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

another certificate, e.g. issued by a TTP) and then checking the fingerprint through telephone, or sending the certificate through courier which authenticates the sender.

The key token verification shall be done using fingerprint of the root certificate based on the algorithms defined in ISO 12855:2015 if ISO/IEC 11770-3 public key transport mechanism 2 is used.

5.4.2 Trust relation renewal and revocation

The root certificate shall have a validity and key length recommended for the use during the planned contract duration between TC and TSP.

NOTE For recommended key length and validity periods, see, for example, https://www.bsi.bund.de/DE/Themen/weitereThemen/ElektronischeSignatur/TechnischeRealisierung/Kryptoalgorithmen/kryptoalgorithmen_node.html (German only).

The trust relation shall automatically end when a root certificate is not replaced by the date of expiry.

The replacement of a root certificate shall be done in the same way as already defined in 5.4.1. All issued end-entity certificates of this root certificate shall be renewed according to the process defined in 5.4.3.

It shall be possible to revoke a root certificate by its issuer before the expiry of the validity for any reason. The revocation of a root certificate shall be done by a procedure similar to the early termination of the contract and results in a termination of the trust relation. The trust relation shall automatically end when a root certificate is revoked.

The information about revocation of a root certificate shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8 signed by the private-key of the root certificate. The digital signature of the message shall be verified with the public key of the originally imported root certificate.

Further activities that are necessary to handle compromised root certificates are beyond the scope of this Technical Specification because they usually require certain organizational measures.

5.4.3 Issuing and revocation of sub CA and end-entity certificates

The corresponding private-key of the root certificate shall only be used for signing end-entity or sub CA certificates. The purpose and usage of the end-entity certificate (e.g. TC to TSP communication) shall be defined by using the extended key usage extension in the ISO/IEC 9594-8 certificate.

The implementation of the certificate verification process shall support a certificate chain starting from a root certificate and contain at least up to four certificate levels (i.e. Root > CA1 > CA2 > CA3 > End-Entity) signed by a sub CA or end-entity private key.

Each entity shall have at least three different end-entity certificates to be used for

— secure communication channels,

— message signing, and

— message or key encryption purposes.

It is recommended that these end-entity certificates have a validity period of less than two years.

The information about revocation of an end-entity certificate shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8 signed by the private-key of the root certificate. The digital signature of the message shall be verified with the public key of the originally imported root certificate.

Exchange of certificates and CRLs is defined in Clause 9.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

5.4.4 Certificate and certificate revocation list profile and format

The issued ISO/IEC 9594-8 certificates version 3 and CRL version 2 shall be according to the profile defined in IETF RFC 5280 with the update specified in RFC 6818. A compliant implementation to this specification to import and use the certificates and CRLs shall at least support all possible critical certificate and CRL extensions as defined in IETF RFC 5280 profile with the update specified in RFC 6818.

All root, sub CA, and end-entity certificates shall be encoded according to the distinguished encoding rules (DER) as defined in ISO/IEC 8825-1 and thereafter, be Base64-encoded as defined in IETF RFC 4648 and enclosed by „–––BEGIN CERTIFICATE–––“ and „–––END CERTIFICATE–––“, i.e. as defined in the PEM (privacy enhanced mail) certificate format.

All CRL shall be DER encoded as defined in ISO/IEC 8825-1 and thereafter, be Base64-encoded (as defined in IETF RFC 4648) and enclosed by „–––BEGIN X.509 CRL–––“ and „–––END X.509 CRL–––“, i.e. as defined in the PEM CRL format.

All certificates and CRL shall have a fingerprint in hexadecimal format based on the algorithms defined in ISO 12855:2015.

5.4.5 Certificate extensions

Considering IETF RFC 5280:2008, 4.2 and clarifications in ISO/IEC 9594-8:2014, Clause 7, the processing of critical extensions is delicate and shall be clearly agreed between the stakeholders (TC and TSP) to avoid implementation problems when the involved PKI platform technologies do not support the processing of certificates with certain extensions marked as critical.

Each extension used in a certificate shall be designated as either critical or non-critical. A certificate-using system shall reject the certificate if it encounters a critical certificate extension it does not recognize or a critical certificate extension that contains information it cannot process. A non-critical extension may be ignored if it is not recognized, but shall be processed if it is recognized.

NOTE Any extension that is flagged non-critical can cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using systems that do not recognize the extension and will ignore it.

A root certificate shall only use the certificate extensions listed below marked as critical:

a) key usage;

b) basic constraints.

An end-entity certificate shall use the certificate extensions listed below marked as critical:

a) key usage;

The values in Table 1 shall be used.

b) Extended key usage with object identifier (OID) for the following:

— TC to TSP interface certificate;

— Front end to TSP back end interfaces certificate.

The following extensions may be present in root certificates as non-critical:

a) CRL distribution points;

b) authority information access.

The following extensions may be present in end-entity certificates as non-critical:

a) basic constraints;

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

b) CRL distribution points;

c) authority information access.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 1 — Values for key usage

Value	Meaning
0	Digital signature
1	Content commitment
2	Key encipherment
3	Data encipherment
4	Key agreement
5	Key certificate signing
6	CRL signing
7	Encipher only
8	Decipher only

6 Security requirements

6.1 General

A security requirement is a functional or non-functional requirement that needs to be satisfied in order to mitigate the threats to an EFC system or reducing its consequences.

Security requirements can be motivated by different sources. The following list presents some of the most relevant sources for EFC systems:

— generic information technology security requirements can be found in ISO Information Security Management System family of standards (e.g. in ISO/IEC 27001);

— security requirements for the protection of payment card data can be found in the Payment Card Industry Data Security Standard (PCI DSS),[12] if applicable;

— system-specific security requirements based on a threat analysis of the EFC system as presented in this Technical Specification in Annex D.

Mainly motivated by the threat analysis in Annex D, the following section specifies a basic set of information security requirements to protect the threatened assets in an EFC system.

The security policy for an EFC scheme or for an EFC operators system may consider additional security requirements driven by the mentioned standards or other relevant sources.

NOTE A general and complete IT security guideline for an information security management system is provided in the ISO 2700x family of standards (see 1.2 and 6.2).

In order to be compliant with this Technical Specification, an implementation shall fulfil all requirements selected in accordance with the applicable security policy. Any security measures from Clause 7 that are associated to the security requirements listed in this Clause shall be implemented when the relevant requirement is selected to be fulfilled.

If a requirement is not selected, it is also not mandatory to implement the associated security measure. In addition to the security policy, there are also some security profiles defined in Annex A to ease the implementation of a common set of security requirements. If an entity states compliance with one or more of the defined security profiles, all mentioned requirements are mandatory and the associated security measures have to be implemented.

Table 2 explains the notation of the requirements defined in this clause.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 2 — Notation of requirements

Table header	Meaning
No.	Unique number for every requirement to enable a later matching with the security measures.
Requirement	Definition of the requirement or recommendation.
DSRC	Marked with an X if this requirement is relevant for a DSRC system.
GNSS	Marked with an X if this requirement is relevant for an autonomous system.

Annex D provides a reference to the requirement(s) that is (are) driven by a given threat.

6.2 Information security management system

This Technical Specification provides measures to address potential EFC specific risks by defining requirements and detailed security measures which take into consideration the specific nature of EFC systems including their interoperable interfaces and specific assets. Those security measures have been designed based on an analysis of possible threats specifically applicable to EFC systems, without evaluating the real associated risks, which are system specific.

TCs and TSPs shall analyse and evaluate the risks associated with those threats and should also identify and analyse more generic information and communication technology risks applicable to organizations operating EFC systems, by performing a comprehensive risk analysis according to ISO/IEC 27005.

In order to effectively ensure information security in a holistic approach, TCs and TSPs shall establish, implement, operate, monitor, review, maintain, and continuously improve an Information Security Management System (ISMS) according to ISO/IEC 27001. The ISMS shall consider the EFC business processes specified in ISO 17573 within its scope and consider, among others, the risks identified in this Technical Specification. The security measures defined in this Technical Speciation shall be used while defining and implementing the controls for minimizing the impact of the identified risks.

The ISMS should also consider the generic companies business processes as part of its scope.

Table 3 — ISMS requirements

No.	Requirement	DSRC	GNSS
RQ.ISMS.1	An Information Security Management System (ISMS) according to ISO/IEC 27001 shall be established, implemented, operated, maintained, and continuously improved.	X	X
RQ.ISMS.2	Non-EFC specific threats shall be covered by a security measure or security control defined by the ISO/IEC 27002 or equivalent standard.	X	X

6.3 Communication interfaces

Communication interfaces are some of the most threatened links in the security chain of the EFC system as shown in the threat analysis in Annex D. Protecting interfaces against all threats without a basic risk analysis results in unreasonably high implementation costs. Table 4 lists all requirements identified in the threat analysis.

Table 4 — General interface requirements

No.	Requirement	DSRC	GNSS
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.	X	X
RQ.IF.10	Data exchange shall guarantee data confidentiality.	X	X
RQ.IF.11	Data exchange shall guarantee data integrity.	X	X

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 4 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.	X	X
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.	X	X
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.	X	X
RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.	X	X
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against replay attacks).	X	X
RQ.IF.31	Data exchange shall allow the detection of mass rejection of toll declarations (protection against interface errors).	X	X
RQ.IF.32	Data exchange shall allow the detection of mass rejection of billing details (protection against interface errors).	X	X

6.4 Data storage

Data storage shall fulfil the following requirements independently of the state of data processing.

Table 5 — Data storage requirements

No.	Requirement	DSRC	GNSS
RQ.DS.01	Access to stored data shall only be granted after authorization.	X	X
RQ.DS.02	Access to stored data shall only be granted via defined interfaces and defined procedures.	X	X
RQ.DS.03	Stored data shall have an independent backup storage.	X	X
RQ.DS.05	Data storage shall guarantee data integrity.	X	X
RQ.DS.06	Access to data storage shall guarantee data confidentiality.	X	X
RQ.DS.07	Data storage shall guarantee non-repudiation with proof of origin for applicable data.	X	X
RQ.DS.08	Data storage shall guarantee non-repudiation with proof of delivery for applicable data.	X	X

6.5 Toll charger

The following clauses list requirements for protection of the TCs assets.

Table 6 — Toll charger requirements

No.	Requirement	DSRC	GNSS
RQ.TC.01	The TC shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations either acquired directly through the TCs RSE or through a TSP (enabled by RQ.TSP.51 for autonomous systems).	X	X
RQ.TC.02	In case the TC performs spot checks, he shall be able to determine the OBE working status (enabled by RQ.TSP.53 for autonomous systems).	X	X
RQ.TC.03	In case the TC performs spot checks, he shall be able to determine the ICC working status in the OBE.	X	X
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the OBE.	X	X
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate OBE or TSP back end (enabled by RQ.TSP.55).	X	X

© ISO 2015 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 6 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TC.06	The TC shall make sure that any invoices generated in his name and on his behalf are conformant to the invoicing rules of his country (enabled by RQ.TSP.56).	X	X
RQ.TC.07	The TC shall ensure that the TSPs OBE is suitable for use in his toll.	X	X
RQ.TC.08	The TC shall check the model and make of OBE during a vehicle check (enabled by RQ.TSP.58) to identify the use of OBE versions not certified by the TC.	X	X
RQ.TC.10	The TC shall implement all necessary technical and organizational mechanisms for a correct implementation of a keyset for OBE communication provided by the TSP.	X	X
RQ.TC.12	The TC shall make sure that his back end system can cope with a sudden change of the customization information of an OBE (e.g. change of license plate over the air).	X	X
RQ.TC.13	The TC shall verify the correctness of billing details received from the TSP. NOTE This requirement is not applicable where the billing details are provided by the TC (this is covered by RQ.TSP.12).	n.a.	X
RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality within an agreed time frame.	X	X
RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part within an agreed time frame.	X	X
RQ.TC.22	The TC shall implement RSE authentication measures for DSRC communication based upon security level 1 as defined in EN 15509:2014 or equivalent national standards/regulations.	X	X
RQ.TC.23	The TC shall detect RSE malfunction or underperformance and correct it within an agreed time frame.	X	X
RQ.TC.24	The RSE shall not allow unauthorized access to software and data.	X	X
RQ.TC.25	The TC shall guarantee confidentiality, integrity, and non-repudiation with proof of origin of a keyset for OBE communication during transfer to the RSE.	X	X
RQ.TC.30	The TC shall implement all necessary technical and organizational measures to avoid an enforcement case when a correct toll declaration was received.	X	X
RQ.TC.31	The TC shall make sure that the correct service user is charged for an enforcement case.	X	X
RQ.TC.32	The TC shall make sure that the enforcement case data are court proof.	X	X
RQ.TC.50	A data protection commissioner or delegate shall have the possibility to audit the system for compliance with data privacy regulations. NOTE Such audits shall be used to prove the data protection concept.	X	X
RQ.TC.51	The TC shall publish his procedures of collecting and processing personal data or register with the responsible data protection authorities.	X	X
RQ.TC.70	The TC shall exhaustively test all features of an RSE update before it is implemented.	X	X
RQ.TC.71	The TC shall have a rollback scenario ready before an RSE update is implemented.	X	X
RQ.TC.90	The TCs systems shall be designed in a way that access to stored or processed data is only possible within the legal context of the respective country (e.g. lawful interception).	X	X
RQ.TC.91	The TC shall provide non-repudiation with proof of origin for distributed toll context data.	X	X

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 6 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific OBE (enabled by RQ.TSP.62).	X	X
RQ.TC.93	The TC shall only accept an OBE after detecting if the ICC in the OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific ICC.	X	X
RQ.TC.94	The TC shall only accept an exception list after verification of non-repudiation with proof of origin.	X	X
RQ.TC.95	The TC shall be responsible for the availability of his back office interfaces according to agreed service levels.	X	X
RQ.TC.96	The TC shall be responsible for the availability of his RSE interfaces to an OBE according to agreed service levels.	X	X
RQ.TC.97	The TC shall verify the provided non-repudiation with proof of delivery in the TSPs acknowledge for distributed toll context data.	X	X
RQ.TC.98	The TC shall implement all necessary technical and organizational measures to guarantee the distribution of correct toll context data to the TSP.	X	X
RQ.TC.99	The TC shall acknowledge a received exception list and provide non-repudiation with proof of delivery to the TSP.	X	X

6.6 Toll service provider

The following clauses list requirements for the protection of the TSPs assets.

Table 7 — Toll service provider requirements

No.	Requirement	DSRC	GNSS
RQ.TSP.01	The TSP shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations.	n.a.	X
RQ.TSP.03	The TSP shall check the integrity and authenticity of the received road usage data sent from the OBE.	n.a.	X
RQ.TSP.04	The TSP shall determine if toll declarations are based on data originating from a legitimate OBE or ICC.	X	X
RQ.TSP.05	The OBE shall prevent or detect illegal modification of parameters through its external interfaces.	X	X
RQ.TSP.06	The ICC shall prevent or detect illegal modification of parameters through its external interfaces.	X	X
RQ.TSP.07	The OBE shall not allow the service user to modify fixed vehicle parameters.	X	X
RQ.TSP.08	The TSP shall detect duplicate or false OBE or ICC identities and block such OBE or ICC identities by placing them on the exception list.	X	X
RQ.TSP.09	The TSP shall notify the service user if the OBE or ICC is not working correctly.	X	X
RQ.TSP.10	The TSP shall determine if billing details are based on correct and complete road usage data.	n.a.	X
RQ.TSP.11	The TSP shall determine if factual road usage is represented by a corresponding set of billing details.	n.a.	X
RQ.TSP.12	The TSP shall verify the correctness of billing details received from the TC. NOTE This requirement is not applicable where the billing details are provided by the TSP (this is covered by RQ.TC.13).	X	X

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 7 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TSP.13	The TSP shall accept received toll context data only after verification of non-repudiation with proof of origin.	X	X
RQ.TSP.14	The TSP shall provide exception lists including non-repudiation with proof of origin to the TC.	X	X
RQ.TSP.16	The OBE shall detect signal input inconsistencies.	n.a.	X
RQ.TSP.17	The TSP shall acknowledge received toll context data and provide non-repudiation with proof of delivery to the TC.	X	X
RQ.TSP.18	The TSP shall verify the provided non-repudiation with proof of delivery in the TCs acknowledge for a distributed exception list.	X	X
RQ.TSP.19	The TSP shall notify the TC about stolen or cloned OBE or ICC.	X	X
RQ.TSP.20	The TSP shall accept reports of stolen OBE or ICC by service users.	X	X
RQ.TSP.21	The TSP shall detect cloned OBE or ICC and block them by placing them on the exception list.	X	X
RQ.TSP.40	The OBE shall not allow change of internal data through the user interface except the data allowed to be changed.	X	X
RQ.TSP.41	The OBE shall only present intended data by the user interface.	X	X
RQ.TSP.42	The TSPs implementation of the front end and gathering and processing of data should be in compliance with the privacy requirements of the toll domain.	X	X
RQ.TSP.50	The TSP shall ensure that only authenticated service users have access to systems that manage their personal data.	X	X
RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of correct and complete toll declarations sent either directly from the OBE to the TCs RSE (in a DSRC system) or through a back office data exchange (required to enable RQ.TC.01 for autonomous systems).	X	X
RQ.TSP.53	The TSP shall enable the TC to perform spot checks through CCC (required to enable RQ.TC.02 for autonomous systems).	X	X
RQ.TSP.55	The TSP shall enable the TC to determine if toll declarations are based on data originating from a legitimate front end (required to enable RQ.TC.05 for autonomous systems) or OBE (in a DSRC system).	X	X
RQ.TSP.56	The TSP shall enable the TC to audit invoices to service users for tolls of his toll domain (required to enable RQ.TC.06).	X	X
RQ.TSP.57	The TSP shall enable the service user to check the correctness of an invoice.	X	X
RQ.TSP.58	The TSP shall enable the TC to check the model and make of OBE during a vehicle check (required to enable RQ.TC.08). NOTE The data in the relevant fields are set by the manufacturer during production. The responsibility of the TSP is to provide the TC with the different possible values for these fields to distinguish between the different OBE models and makes.	X	X
RQ.TSP.59	The TSP shall publish his procedures of collecting and processing personal data or register with the responsible data protection authorities.	X	X
RQ.TSP.60	The TSP shall only use equipment that passed certification by the TC and delivers the agreed quality of service.	X	X
RQ.TSP.62	The TSP shall enable the TC to detect if an OBE belongs to the TSP (required to enable RQ.TC.92).	X	X
RQ.TSP.70	The TSP shall exhaustively test all features of an OBE update before it is implemented (e.g. distributed over the air).	X	X

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 7 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TSP.71	The TSP shall have a rollback scenario ready before an OBE update is implemented (e.g. distributed over the air).	X	X
RQ.TSP.80	The TSP shall implement all necessary technical and organizational quality control mechanisms for all OBE before they are distributed to the service users.	X	X
RQ.TSP.81	The TSP shall implement all necessary technical and organizational quality control mechanism for the provision of a key set for OBE communication to the TC.	X	X
RQ.TSP.82	The TSP shall implement all necessary technical and organizational quality control mechanism for the maintenance or exchange of OBE with low performance.	X	X
RQ.TSP.89	The TSP shall take protective measures against repudiation of invoices and its underlying confirmation data by service users.	X	X
RQ.TSP.90	The TSPs systems should be designed in a way that access to stored or processed data is only possible within the legal context of the respective countries (lawful interception).	X	X
RQ.TSP.91	The data communication between front end (OBE) and back end (TSP) shall be protected against interception in a way that access to stored or processed data is only possible within the legal context of the respective country (lawful interception).	n.a.	X
RQ.TSP.92	Customization of OBE shall be done in a secure way to guarantee data integrity and non-repudiation with proof of origin.	X	X
RQ.TSP.96	The TSP shall guarantee the availability of its POS network according to agreed service levels.	X	X
RQ.TSP.97	The TSP shall implement all necessary technical and organizational measures that an update of the customization information is correct.	X	X

6.7 Interoperability Management

The main security requirement for an interoperability management is to ensure the trust of all stakeholders in the interoperability scheme.

Table 8 — Interoperability management requirements

No.	Requirement	DSRC	GNSS
RQ.IM.01	The interoperability management shall issue an EFC security policy. NOTE Examples explaining the content of such a security policy are given in Annex E and Annex F.	X	X
RQ.IM.02	The interoperability management shall have or define one or more auditing bodies supervising the security implementation of the TSP and TC involved in the interoperable EFC scheme.	X	X

6.8 Limitation of requirements

The following requirements are included to document the limitation of security measures against some threats. This means that either no required security measure exists to protect against the threat, or the security measure is not really feasible because it is much too expensive. The requirements in Table 9 are not further treated in this Technical Specification.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 9 — Denial of service and hardware integrity threats

No.	Requirement	DSRC	GNSS
RQ.XX.01	Prevent denial of service attack. Prevent message transmission delay. This requirement covers attacks against a communication interface or against a whole service. A simple and/or cheap security measure does not exist due to the fact that long distance communication interfaces cannot be protected against all kinds of imaginable attacks.	X	X
RQ.XX.02	Prevent manipulating equipment; especially prevent OBE from HW manipulation. Such a requirement can be fulfilled by developing a tamperproof OBE, which is not deemed viable from a cost efficiency perspective.	X	X

7 Security measures — countermeasures

7.1 Overview

A security measure describes actions to be taken by the addressed entity to satisfy one or more security requirements. The actual implementation of the action is up to the entity. A security measure describes one possible solution to satisfy one or more security requirements.

In order to be compliant with this Technical Specification, an implementation shall fulfil all security measures that are associated to the security requirements in Clause 6 which are selected in accordance with the applicable security policy.

The table below explains the notation and relations of the security measures defined in this Clause.

Table 10 — Notation and relations of security measures

Table header	Meaning
No.	Unique number for every security measure
Security measure	Description of the security measure (countermeasure)
DSRC	Marked with an X if this security measure is relevant for a DSRC system
GNSS	Marked with an X if this security measure is relevant for an autonomous system
Fulfilled RQ	List of requirements that the security measure fulfils

NOTE For a detailed definition for the implementation of communication interface security measure, see Clause 8.

7.2 General security measures

This Technical Specification provides measures to address potential EFC specific risks by defining requirements and detailed security measures which take into consideration the specific nature of EFC systems including their interoperable interfaces and specific assets. Those security measures have been designed based on an analysis of possible threats specifically applicable to EFC systems, without evaluating the real associated risks, which are system specific.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 11 — General security measures

No.	Security measure	DSRC	GNSS
		Fulfilled RQ	
SM.101	The TC shall register the data processing application of the EFC system with the national data protection commissioner or authority for compliance with national data protection regulations if required by law.	X	X
		RQ.TC.50 RQ.TC.51 RQ.TSP.42 RQ.TSP.59 RQ.TSP.90 RQ.TSP.91	
SM.102	The TC and the TSP shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement, the duties and rights of the TSP are stated in regard to the data processing.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
		RQ.TC.06 RQ.TSP.56 RQ.TSP.89	
SM.103	The contracting parties of communication providers shall sign a Personal Data Assistant Agreement or equivalent to be compliant to the national data protection regulations of the TC. In this agreement, the duties and rights of the communication provider are stated in regard to the processing of personal data.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
SM.104	The TC shall have the possibility to perform audit(s) of the TSP systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
SM.105	The contracting parties of communication providers shall have the possibility to perform audit(s) of the communication providers systems and procedures to prove the adherence to the registered data processing application and the Personal Data Assistant Agreement or equivalent.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
SM.106	The TSP shall establish a quality control process for the maintenance or exchange of low performing OBE within an agreed time frame. This process may be initiated by the detection of a low performing OBE by the TSP or by a report of such an OBE by the TC.	X	X
		RQ.TSP.82	
SM.107	The TSP shall enable the TC to audit invoices generated in his name. The TC shall periodically audit invoices to service users for tolls of his toll domain.	X	X
		RQ.TC.06 RQ.TSP.56 RQ.TSP.89	

7.3 Communication interfaces security measures

7.3.1 General

Security measures for the protection of data exchanged between entities using the different interfaces.

Table 12 — General interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.200	The contracting parties of communication providers shall have proper service levels agreed and monitoring procedures in place that are able to detect any non-compliant behaviour of the communication provider.	X	X
		RQ.IF.02 RQ.TSP.60	

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: PD CEN ISO/TS 19299:2015

Table 12 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.201	The TC and the TSP shall agree on defined interfaces and procedures for the access to stored data. These interfaces should be based on European or International Standards whenever possible.	X	X
		RQ.DS.02 RQ.DS.06 RQ.IF.20 RQ.IF.31 RQ.IF.32 RQ.TC.24 RQ.TC.90	
SM.202	The TC and the TSP shall only allow access to stored data for an authorized and authenticated entity.	X	X
		RQ.DS.01 RQ.IF.20 RQ.TC.24 RQ.TC.90 RQ.TSP.50	
SM.203	Implement the security measure or security control defined by ISO/IEC 27002 or equivalent.	X	X
		RQ.DS.03 RQ.DS.05 RQ.ISMS.2	
SM.204	The TC and TSP shall agree on a service level agreement defining quality goals and response times.	X	X
		RQ.TC.07 RQ.TC.20 RQ.TC.21 RQ.TC.23 RQ.TC.95 RQ.TC.96 RQ.TSP.60 RQ.TSP.96	
SM.205	Implement an Information Security Management System (ISMS) according to ISO/IEC 27001 or an equivalent.	X	X
		RQ.ISMS.1	
SM.207	Proof of origin authenticators shall be stored together with the data received.	X	X
		RQ.DS.07	
SM.208	Proof of delivery authenticators shall be stored together with the data delivered.	X	X
		RQ.DS.08	

7.3.2 DSRC-EFC interface

Table 13 — DSRC-EFC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.210	If toll declarations are acquired through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TC (MAC_TC) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TC and the TSP during an EFC transaction. The OBE shall respond accordingly.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TSP.55 RQ.TSP.89	

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 13 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.211	If toll declarations are acquired through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TSP (MAC_TSP) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TSP during an EFC transaction. The OBE shall respond accordingly.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.04 RQ.TSP.89	
SM.212	The OBE shall implement an access control mechanism for an EFC command addressing its EFC data attributes. The RSE shall implement the calculation of the corresponding access codes.	X	n.a.
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	
SM.213	The RSE shall read, increment, and write a transaction counter to the OBE. The OBE shall support this.	X	n.a.
		RQ.TSP.21	
SM.214	The TSP shall implement a MAC_TSP authenticator in the OBE to prove its authenticity and integrity.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.03 RQ.TSP.04 RQ.TSP.62	
SM.215	The TSP shall implement a MAC_TC authenticator in the OBE to prove its authenticity and integrity.	X	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.62	

7.3.3 CCC interface

Table 14 — CCC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.220	If compliance checking is performed through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TC (MAC_TC) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TC and the TSP during a CCC transaction. The OBE shall respond accordingly.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.53	
SM.221	If compliance checking is performed through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TSP (MAC_TSP) over at least the PaymentMeans attribute, using a key known only to the TSP during a CCC transaction. The OBE shall respond accordingly.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13	

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 14 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.222	The OBE shall implement an access control mechanism for an EFC command addressing its CCC data attributes. The RSE shall implement the calculation of the corresponding access codes.	n.a.	X
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41 RQ.TSP.53	
SM.223	If toll declarations are acquired by the TSP, the OBE shall provide an undeniable proof of correct registration of road usage data for the given location and moment in time of the CCC transaction.	n.a.	X
		RQ.TC.01 RQ.TSP.51 RQ.TSP.53 RQ.TSP.89	

7.3.4 LAC interface

Table 15 — LAC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.230	If localization augmentation communication is performed through the DSRC interface, the RSE shall provide a MAC_TC over the LAC data sent to the OBE calculated with a key known only to the TC and the lacTime.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13	
SM.231	The OBE shall implement an access control mechanism for an EFC command addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.	n.a.	X
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	

7.3.5 Front End to TSP back end interface

Table 16 — Front end to TSP back end interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.240	The TSP shall implement an authenticator in the charge report which guarantees its authenticity and integrity.	n.a.	X
		RQ.TC.04 RQ.TSP.03	
SM.241	The bidirectional Front End to TSP back end communication shall be implemented using a secure connection.	n.a.	X
		RQ.IF.10 RQ.IF.11	

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

7.3.6 TC to TSP interface

Table 17 — TC to TSP interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.250	The bidirectional TC to TSP back office data exchange shall be implemented using a secure connection with authentication.	X	X
		RQ.IF.10 RQ.IF.11 RQ.IF.31 RQ.IF.32	
SM.251	The TC shall link the billing details to a set of toll declarations provided by the TSP or include the associated event data for those toll declarations which have been acquired by him.	X	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12	
SM.252	If the TSP receives billing details from the TC, he shall compare them against the sent toll declarations to detect modifications and/or missing or additional toll declarations not sent to the TC in a GNSS environment.	n.a.	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12 RQ.TSP.89	
SM.253	Distribution of toll context data shall be undeniably signed by the TC and confirmed by the TSP in an agreed time frame with an authenticated response.	X	X
		RQ.IF.12 RQ.IF.13 RQ.IF.14 RQ.TC.91 RQ.TC.97 RQ.TSP.13 RQ.TSP.17	
SM.254	Distribution of the exception list shall be undeniably signed by the TSP and confirmed by the TC in an agreed time frame with an authenticated response.	X	X
		RQ.IF.12 RQ.IF.13 RQ.IF.14 RQ.TC.94 RQ.TC.99 RQ.TSP.14 RQ.TSP.18	
SM.255	The front end and/or the TSP back end shall undeniably sign charge reports and/or toll declarations.	n.a.	X
		RQ.IF.12 RQ.IF.13 RQ.TSP.55 RQ.TSP.89	
SM.256	The originator of a trust object shall undeniably sign it.	X	X
		RQ.IF.12 RQ.IF.13 RQ.TC.25 RQ.TSP.81	
SM.257	The TSP shall provide data underlying a specific toll declaration acquired through his system on demand of the TC (charge report and/or more detailed road usage data).	n.a.	X
		RQ.TSP.51	
SM.258	The TC shall provide the tariff table and all the relevant toll context data to the TSP to allow him to calculate the amount given in the billing details. NOTE Other means than ISO/TS 17575-3 could be used, e.g. publication on a website.	X	X
		RQ.TC.98 RQ.TSP.12	

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 17 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.259	The TSP shall be able to perform plausibility and completeness checks on received billing details. NOTE Those checks could be performed by the verification of the physical feasibility of trips in the toll domain.	X	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12	
SM.260	The TSP shall establish a control mechanism to ensure a correct provision of a key set for OBE communication to the TC.	X	X
		RQ.TSP.81	
SM.261	The TC and the TSP shall establish a data transfer protocol that allows the detection of duplicate messages as a protection against replay attacks.	X	X
		RQ.IF.30	
SM.262	The TSP shall provide the TC with the data about all valid OBE issued by him.	X	X
		RQ.TSP.55 RQ.TSP.58 RQ.TSP.62	
SM.263	The TC shall verify that an OBE is listed as valid by the TSP who issued it.	X	X
		RQ.TC.08 RQ.TC.92	
SM.264	The TC shall guarantee the correct manual entry or automatic processing of a keyset for OBE communication provided by the TSP.	X	X
		RQ.TC.10	
SM.265	The TC shall compare the billing details received from the TSP against the sent toll declarations to detect modifications, missing, or additional toll declarations not sent to the TC in a GNSS environment.	n.a.	X
		RQ.TC.13 RQ.TSP.89	
SM.266	The TC shall always acquire the correct and current service user details before starting an enforcement procedure.	X	X
		RQ.TC.31	

7.3.7 ICC interface

Table 18 — ICC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.270	The OBE shall calculate an authentication code to ICC complying with ISO/IEC 7816-3 command/response using a key known only to the ICC issuer.	X	X
		RQ.IF.11 RQ.IF.12	

7.4 End-to-end security measures

End-to-end security means front end to TSP to TC security measures.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 19 — End-to-end security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.310	The OBE shall be designed as a clearly distinguished entity with a defined interface to the TC RSE. The OBE's functionality shall be tested to guarantee its functionality and it shall be auditable according to suitability for use procedure.	X	n.a.
		RQ.TC.01 RQ.TC.07 RQ.TC.12 RQ.TSP.51 RQ.TSP.60 RQ.TSP.70	
SM.311	The correct and trustworthy OBE functionality shall be periodically audited by the TSP and optionally by the TC or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with known independent trip data.	X	X
		RQ.TC.01 RQ.TC.07 RQ.TSP.51 RQ.TSP.60	
SM.312	The TC shall perform plausibility and completeness checks on toll declarations acquired by the TSP in a GNSS environment.	n.a.	X
		RQ.TC.01 RQ.TC.12	
SM.313	The TC shall compare toll declarations acquired by the TSP with his own observations in accordance with privacy regulations.	n.a.	X
		RQ.TC.01	
SM.314	The TC shall verify if toll declaration(s) acquired by the TSP correctly correspond(s) to charge report(s) and/or road usage data.	n.a.	X
		RQ.TC.01	
SM.315	The TSP shall prepare a fall back scenario before any OBE update and initiate a rollback of the update when needed.	X	X
		RQ.TSP.71	
SM.316	The TC shall determine if the toll declarations have been produced by a trusted OBE by a message authentication code (MAC) or digital signature.	X	X
		RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TC.04 RQ.TC.05	
SM.317	The TSP shall undeniably sign any update package before it is distributed over the air to ensure its integrity. The OBE shall check the integrity of the received update before the update is started.	X	X
		RQ.TSP.70	
SM.318	If toll declarations are acquired by the TSP, the registration of road usage data shall be based on a minimum set of functions in the OBE trusted by both the TSP and the TC. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.	n.a.	X
		RQ.TC.01 RQ.TC.04 RQ.TC.05 RQ.TSP.51 RQ.TSP.55 RQ.TSP.89	
SM.319	The TSP shall provide an undeniable proof of correct registration of road usage data for a defined location and moment in time or for a defined range of time and for a specified set of OBE(s) on demand to the TC.	n.a.	X
		RQ.TSP.51	
SM.320	The TC shall compare proof of correct registration of road usage data acquired by the TSP with his own observations in accordance with privacy regulations.	n.a.	X
		RQ.TC.01	
SM.322	The OBE shall be designed as a clearly distinguished entity with a defined interface to the proxy or TSPs back end. The OBE's functionality shall be tested to guarantee its functionality and it shall be auditable according to a defined procedure.	n.a.	X
		RQ.TC.07 RQ.TSP.01 RQ.TSP.60 RQ.TSP.70	

Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: PD CEN ISO/TS 19299:2015

Table 19 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.323	The TSP shall perform plausibility and completeness checks on toll declarations acquired by him. Those checks comprise the verification of the physical feasibility of trips in the toll domain compared with the actual toll declarations.	n.a.	X
		RQ.TSP.01 RQ.TSP.51	
SM.324	The TC shall prepare a fall back scenario before any RSE update and initiate a rollback of the update when needed.	X	X
		RQ.TC.71	
SM.330	The TSP shall provide the service user with the detailed transaction data upon request.	X	X
		RQ.TSP.57 RQ.TSP.89	

7.5 Toll service provider security measures

7.5.1 Front end security measures

Table 20 — Front end/OBE interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.410	If compliance checking is performed through the DSRC interface, the OBE shall support a Compliance Checking Communication transaction over an interface with security as defined in ISO 12813:2015 when it passes such a RSE or use secure monitoring-compliance checking.	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.51 RQ.TSP.53	
SM.411	The TSP shall test a significant percentage of OBE delivered to him to achieve an accepted quality level according to ISO 2859 or equivalent.	X	X
		RQ.TSP.80	
SM.412	If localization augmentation communication is performed through the DSRC interface, the TSP shall store the value of the MAC_TC, KeyRef, and lacTime as part of the charge data and provide them as part of the charge report.	n.a.	X
		RQ.IF.12 RQ.IF.13 RQ.TSP.51	
SM.413	The OBE shall implement a role based access control mechanism for its DRSC interface. Any commands reserved to the TSP (i.e. other than those for DSRC-EFC, CCC, and LAC) shall be usable only by the TSP.	X	X
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	
SM.414	The service user shall be notified about the OBE or ICC working status.	X	X
		RQ.TC.02 RQ.TC.03 RQ.TSP.09	
SM.415	The communication between OBE and proxy shall guarantee confidentiality, integrity, and authenticity.	n.a.	X
		RQ.IF.10 RQ.IF.11	
SM.416	The OBE shall prevent any illegal modification of parameters through its external interfaces or switch to a “NOT OK” state if it detects it.	X	X
		RQ.TSP.05 RQ.TSP.07	

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015

Table 20 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.417	The OBE shall switch to a "NOT OK" state if it detects signal input inconsistencies and the TSP shall be informed by the GNSS OBE.	n.a.	X
		RQ.TSP.16	
SM.418	The OBE shall not allow the service user to modify any data in the OBE except the data allowed to be changed through the user interface.	X	X
		RQ.TSP.05 RQ.TSP.07 RQ.TSP.40	
SM.419	The ICC shall not allow the service user to modify any data in the ICC.	X	X
		RQ.TSP.06	

7.5.2 Back end security measures

Table 21 — TSP back end security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.420	The TSP shall verify if toll declaration(s) correctly correspond(s) to charge report(s) and/or road usage data.	n.a.	X
		RQ.TSP.51	
SM.421	The TSP shall determine if the charge report has been produced by a trusted front end.	n.a.	X
		RQ.TSP.01 RQ.TSP.04 RQ.TSP.08	
SM.422	The TSP shall verify the integrity of the charge report.	n.a.	X
		RQ.TSP.01	
SM.423	The TSP shall include stolen or cloned OBE or ICC in an exception list.	X	X
		RQ.TSP.08 RQ.TSP.19 RQ.TSP.20 RQ.TSP.21	
SM.424	The TSP shall detect a cloned OBE or ICC by using the transaction counter or by detecting multiple locations for the same OBE or ICC at the same time.	X	X
		RQ.TSP.08 RQ.TSP.21	
SM.425	The TSP shall use cryptographic measures to encrypt the sending of customization data to the OBE to guarantee data integrity and non-repudiation with proof of origin.	X	X
		RQ.TSP.92 RQ.TSP.97	
SM.426	The TSP shall verify the integrity of the charge report based on the MAC_TSP or digital signature.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.01 RQ.TSP.03 RQ.TSP.04	

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 19299:2015