



SLOVENSKI STANDARD

SIST-TS CEN ISO/TS 19299:2016

01-marec-2016

Nadomešča:

SIST-TS CEN/TS 16439:2013

Elektronsko pobiranje pristojbin - Varnostni okvir (ISO/TS 19299:2015)

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: CEN ISO/TS 19299:2015

<https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3def8e3fba4/sist-ts-cen-iso-ts-19299-2016>

ICS:

35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade
-----------	---	--

SIST-TS CEN ISO/TS 19299:2016

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN ISO/TS 19299:2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)

<https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016>

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.

[SIST-TS CEN ISO/TS 19299:2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)

<https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016>



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

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

Contents	Page
European foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN ISO/TS 19299:2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)
[https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-
b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)

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.

iTeh STANDARD PREVIEW
Endorsement notice
(standards.iteh.ai)

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

[SIST-TS CEN ISO/TS 19299:2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)
<https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN ISO/TS 19299:2016](#)

<https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016>

TECHNICAL
SPECIFICATION

ISO/TS
19299

First edition
2015-10-01

**Electronic fee collection — Security
framework**

Perception de télépéage — Cadre de sécurité

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN ISO/TS 19299:2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)

[https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-
b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)



Reference number
ISO/TS 19299:2015(E)

© ISO 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN ISO/TS 19299:2016](https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016)

<https://standards.iteh.ai/catalog/standards/sist/91b50667-cc96-4d23-bf82-b3dcf8e3fba4/sist-ts-cen-iso-ts-19299-2016>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. (standards.iteh.ai)	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

ISO/TS 19299:2015(E)

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

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/TS 19299:2015(E)

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.

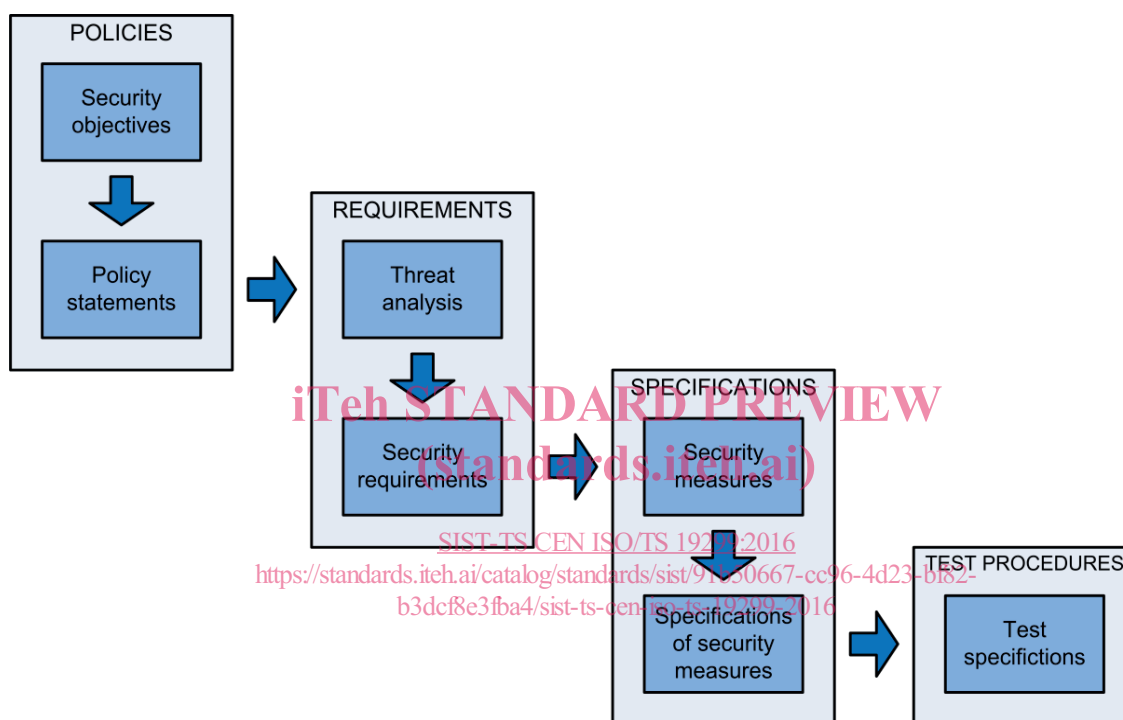


Figure 1 — Development path for the security documents

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.

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

ISO/TS 19299:2015(E)

[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](#)).

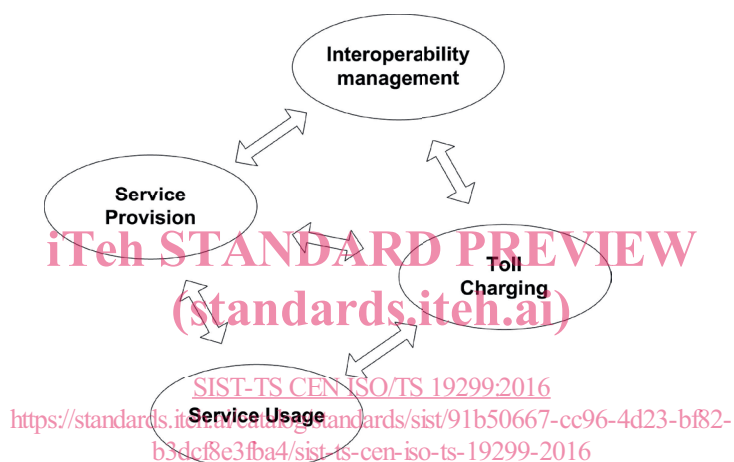


Figure 2 — The role model underlying this Technical Specification

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

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.

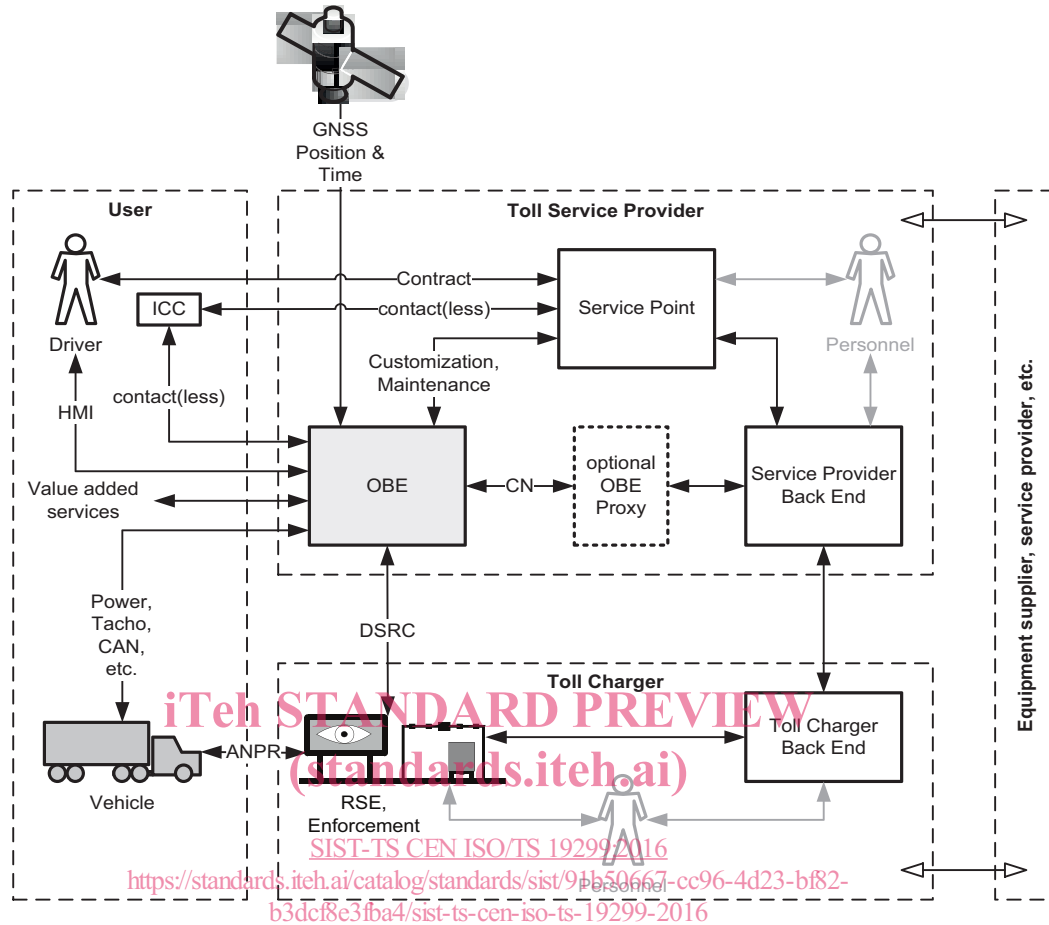


Figure 3 — EFC system model of the EFC Security framework

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.