



**SLOVENSKI STANDARD
SIST EN ISO 19299:2020**

01-november-2020

Nadomešča:

SIST-TS CEN ISO/TS 19299:2016

Elektronsko pobiranje pristojbin - Varnostni okvir (ISO 19299:2020)

Electronic fee collection - Security framework (ISO 19299:2020)

Elektronische Gebührenerhebung - Sicherheitsgrundstruktur (ISO 19299:2020)

Perception de télépéage -- Cadre de sécurité (ISO 19299:2020)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: EN ISO 19299:2020

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debb7b9d/sist-en-iso-19299-2020>

ICS:

35.240.60 Uporabniške rešitve IT v IT applications in transport
 prometu

SIST EN ISO 19299:2020

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 19299:2020

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>

EUROPEAN STANDARD

EN ISO 19299

NORME EUROPÉENNE

EUROPÄISCHE NORM

September 2020

ICS 35.240.60; 03.220.20

Supersedes CEN ISO/TS 19299:2015

English Version

Electronic fee collection - Security framework (ISO 19299:2020)

Perception de télépéage - Cadre de sécurité (ISO 19299:2020)

Elektronische Gebührenerhebung - Sicherheitsgrundstruktur (ISO 19299:2020)

This European Standard was approved by CEN on 10 August 2020.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 19299:2020
<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>

European foreword

This document (EN ISO 19299:2020) 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.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2021, and conflicting national standards shall be withdrawn at the latest by March 2021.

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

This document supersedes CEN ISO/TS 19299:2015.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

The text of ISO 19299:2020 has been approved by CEN as EN ISO 19299:2020 without any modification.

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 19299:2020

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>

INTERNATIONAL
STANDARD

ISO
19299

First edition
2020-08

**Electronic fee collection — Security
framework**

Perception de télépéage — Cadre de sécurité

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 19299:2020](https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020)

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>



Reference number
ISO 19299:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO 19299:2020

<https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	3
5 Trust model	4
5.1 Overview.....	4
5.2 Stakeholders trust relations.....	5
5.3 Technical trust model.....	6
5.3.1 General.....	6
5.3.2 Trust model for TC and TSP relations.....	6
5.3.3 Trust model for TSP and service user relations.....	7
5.3.4 Trust model for interoperability management relations.....	7
5.4 Implementation.....	7
5.4.1 Setup of trust relations.....	7
5.4.2 Trust relation renewal and revocation.....	8
5.4.3 Issuing and revocation of sub CA and end-entity certificates.....	8
5.4.4 Certificate and certificate revocation list profile and format.....	9
5.4.5 Certificate extensions.....	9
6 Security requirements (standards.iteh.ai)	10
6.1 General.....	10
6.2 Information security management system.....	11
6.3 Communication interfaces.....	12
6.4 Data storage.....	12
6.5 Toll charger.....	12
6.6 Toll service provider.....	14
6.7 Interoperability management.....	16
6.8 Limitation of requirements.....	17
7 Security measures — Countermeasures	17
7.1 Overview.....	17
7.2 General security measures.....	18
7.3 Communication interfaces security measures.....	18
7.3.1 General.....	18
7.3.2 DSRC-EFC interface.....	19
7.3.3 CCC interface.....	20
7.3.4 LAC interface.....	21
7.3.5 Front End to TSP back end interface.....	21
7.3.6 TC to TSP interface.....	22
7.3.7 ICC interface.....	23
7.4 End-to-end security measures.....	24
7.5 Toll service provider security measures.....	25
7.5.1 Front end security measures.....	25
7.5.2 Back end security measures.....	26
7.6 Toll charger security measures.....	27
7.6.1 RSE security measures.....	27
7.6.2 Back end security measures.....	28
7.6.3 Other TC security measures.....	28
8 Security specifications for interoperable interface implementation	29
8.1 General.....	29
8.1.1 Subject.....	29

ISO 19299:2020(E)

8.1.2	Signature and hash algorithms.....	29
8.2	Security specifications for DSRC-EFC.....	29
8.2.1	Subject.....	29
8.2.2	OBE.....	29
8.2.3	RSE.....	29
9	Key management.....	30
9.1	Overview.....	30
9.2	Asymmetric keys.....	30
9.2.1	Key exchange between stakeholders.....	30
9.2.2	Key generation and certification.....	30
9.2.3	Protection of keys.....	30
9.2.4	Application.....	31
9.3	Symmetric keys.....	31
9.3.1	General.....	31
9.3.2	Key exchange between stakeholders.....	31
9.3.3	Key lifecycle.....	32
9.3.4	Key storage and protection.....	33
9.3.5	Session keys.....	34
Annex A (normative) Security profiles.....		35
Annex B (informative) Implementation conformance statement (ICS) proforma.....		39
Annex C (informative) Stakeholder objectives and generic requirements.....		57
Annex D (informative) Threat analysis.....		61
Annex E (informative) Security policies.....		118
Annex F (informative) Example for an EETS security policy.....		124
Annex G (informative) Recommendations for privacy-focused implementation.....		126
Bibliography.....	https://standards.iteh.ai/catalog/standards/sist/0c4831b6-dd62-42ee-9e5a-58debeb7b9f9/sist-en-iso-19299-2020	128

Foreword

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

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 ISO documents 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 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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 278 *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition cancels and replaces ISO/TS 19299:2015, which has been technically revised.

The main changes compared to the previous edition are as follows:

- added requirements and security measures for the use of common payment media according to ISO/TS 21193;
- updated data protection considerations in [Annex G](#), in order to take into account the European Union's new General Data Protection Regulation (i.e. Directive 2016/679/EC).

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

ISO 19299:2020(E)

Introduction

Context of this document

The development process for a security concept and implementation to protect any existing electronic fee collection (EFC) system normally includes several steps as follows (see [Figure 1](#)):

- 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.

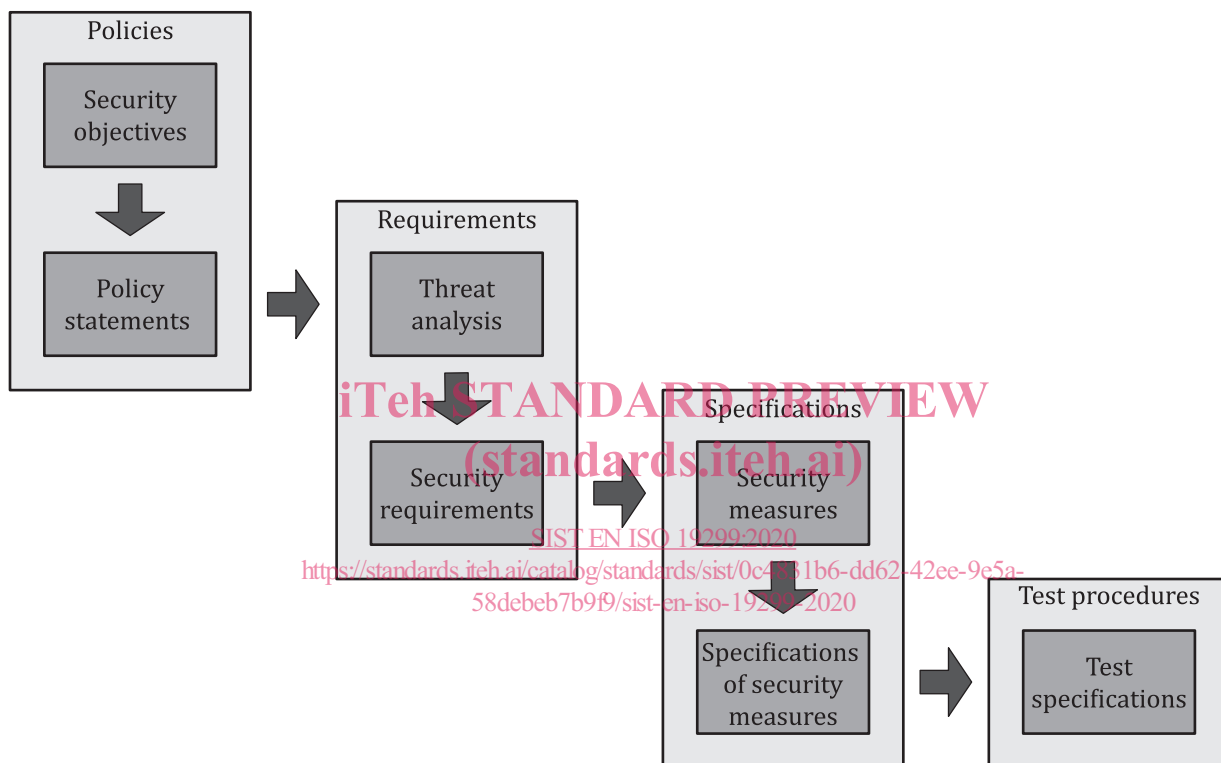


Figure 1 — Development path for the security documents

Each actor in an existing EFC system implements the defined security measures and supervises their effectiveness. When a security measure is found not working properly, an improvement process is started. The development of the EFC security framework follows this approach, with the following limitations:

- No standard security policy exists, nor can it be defined: The security policy can only be defined by the responsible stakeholders and it is limited by laws and regulations. Nonetheless, this document provides basic examples of possible security policies (in [Annex E](#) to [Annex F](#)).
- No standard risk assessment is possible: Risk assessment compares possible losses to stakeholders with the required resources (e.g. equipment, knowledge, time) to perform an attack. In a real system, risk assessment is based on the evaluation of the costs and benefits of each countermeasure.
- No specific system design or configuration was deemed as universally applicable. Only the available EFC base standards were taken as references. Specific technical details of a particular system (e.g. servers, computer centres, and de-centralised elements like roadside equipment) need to be additionally taken into consideration when implementing security measures.

Selection of requirements and 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 no overall valid security policy, nor is there the possibility to provide a useful risk assessment, the EFC security framework provides an extensive (but non-exhaustive) toolbox of requirements and security measures.

To understand the content of this document, the reader should be aware of the methodological assumptions used to develop it. 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. An application independent security framework for such system parts and interfaces, an information security management system (ISMS), can be found, for example, in the ISO/IEC 27000 series.

The development process of this document 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 a 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 17573-1), 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 several threat scenarios from the perspective of various attackers. The second approach looks in depth on threats against the various identified assets (tangible and intangible). This approach, although producing some redundancy, ensures completeness and coverage of a broad 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 each threat is covered by at least one requirement.
- 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, such as 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 (e.g. keys, certificates, certificate revocation lists) to support security services like confidentiality, integrity, authenticity, and non-repudiation. This section of the document covers the (initial) setup of key exchange between stakeholders and several operational procedures, such as key renewal, certificate revocation.
- 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 should 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 [Annex E](#) and [Annex F](#)) as an aid to build up a secure system for a concrete interoperability framework (including the European electronic toll service).

ISO 19299:2020(E)

- 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 of this document. Evidence can be provided by a self-declaration, an internal or external audit, or other certifications.

EFC role model

This document complies with the role model defined in ISO 17573-1. According to this role model, the toll charger (TC) manages the tolled infrastructure or transport service and is the recipient of the road usage fees. The TC is the actor associated with the toll charging role (see [Figure 2](#)).

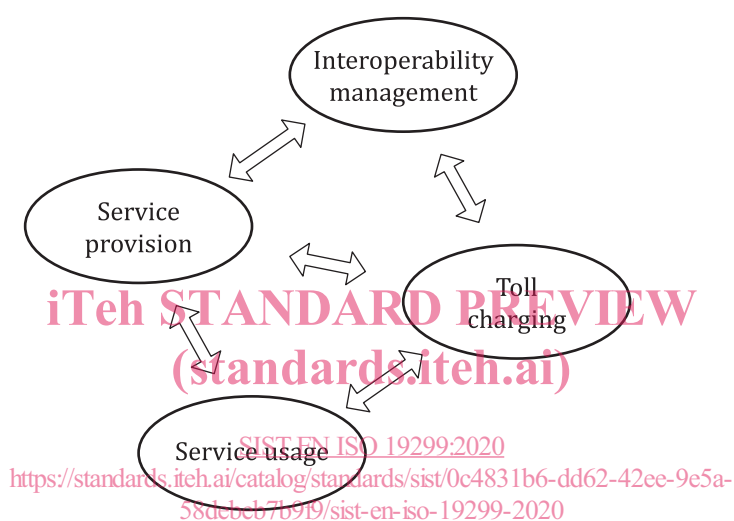


Figure 2 — Role model underlying this document

Toll service providers (TSPs) act as intermediaries between TC's and road users, by providing these latter with contractual relationships and devices (generally on-board equipment — OBE) to interface the tolled infrastructure or transport service. The OBE 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. 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. The interoperability management role (IM) in [Figure 2](#) comprises all specifications and activities that define and maintain a set of rules that govern the overall toll charging environment.

The trust model defined in this document is based on the role model summarized 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 essential. A TC or TSP compliant to this document should 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 and define the security requirements and associated security measures for this document. This document assumes an OBE that is dedicated to EFC purposes only and does not consider value added services based on EFC OBE, nor does it consider more generic OBE platforms (also called in-vehicle ITS Stations) which could be used to host the EFC application. The OBE may either be connected to a central account or use a payment medium such as integrated circuit cards (ICC) or mobile payment for on-board-account EFC system. Any financial transactions are out of scope of this document.

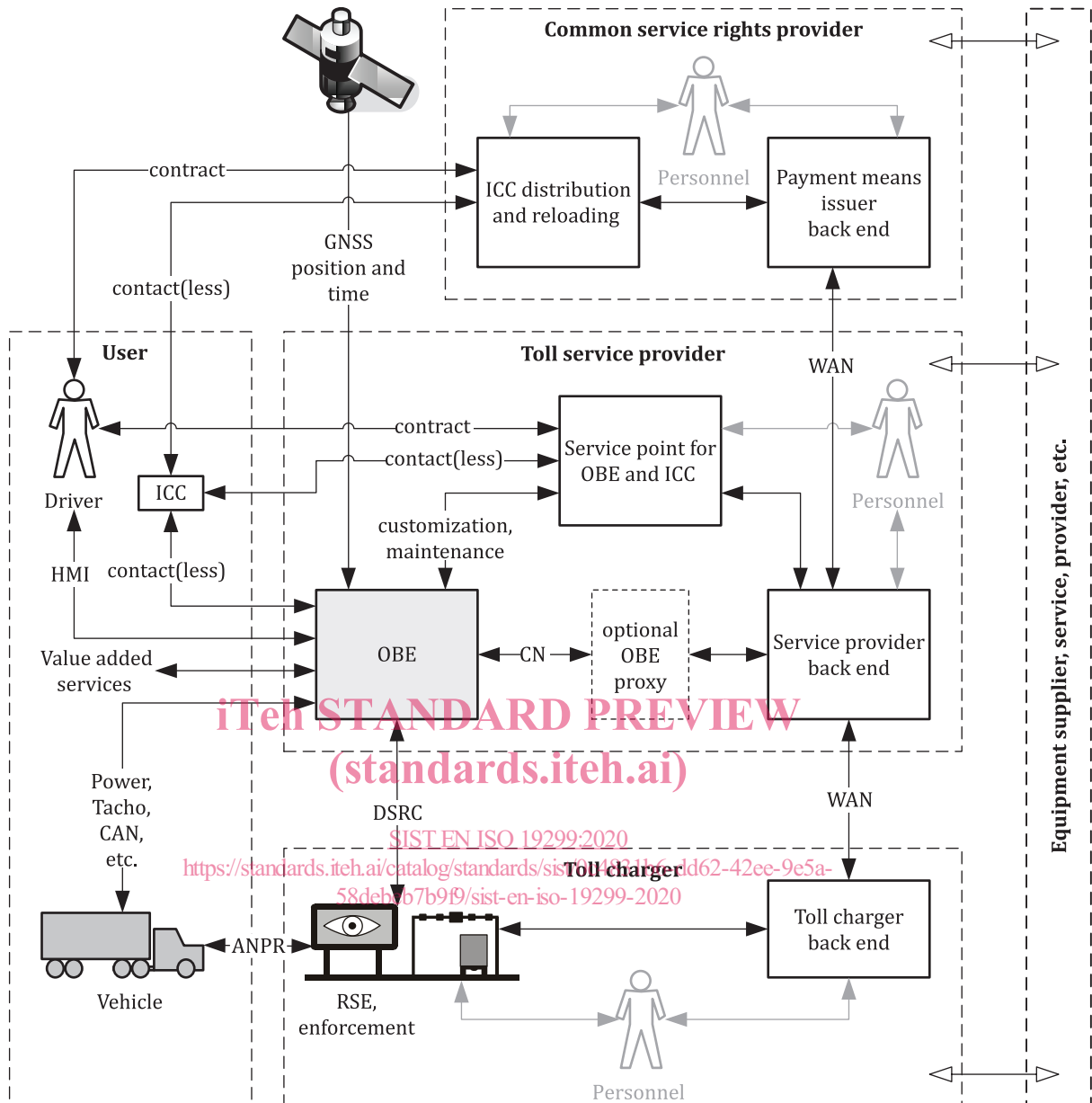


Figure 3 — EFC system model of the EFC security framework

Relation to other security standards

Several generic and specific standards and technical reports concerning security issues for information technology already exist. This document makes use of existing standards and expands their usability for EFC applications. This framework references and adapts security techniques and methodologies from relevant standards.

Figure 4 shows the context of the EFC security framework to the most relevant security standards that gave input to this document. Standards that are directly used and referenced are highlighted in black.