BS EN ISO 19299:2020

BSI Standards Publication

Electronic fee collection – Security framework

Documents
Document Sharing Hub

Full document details: BS EN ISO 19299:2020

National foreword

This British Standard is the UK implementation of EN ISO 19299:2020. It is identical to ISO 19299:2020. It supersedes PD CEN ISO/TS 19299:2015, which is withdrawn.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 committee manager.

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 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 04800 1

ICS 03.220.20; 35.240.60

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN ISO 19299:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 19299

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.

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

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

© 2020 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN ISO 19299:2020 E

Documents
Document Sharing Hub

Full document details: BS 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.

Endorsement notice

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

Documents
Document Sharing Hub

Full document details: BS EN ISO 19299:2020

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 ... **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

AVA Documents
Document Sharing Hub

© ISO 2020 – All rights reserved

Full document details: BS EN ISO 19299:2020

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 ... 128

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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.

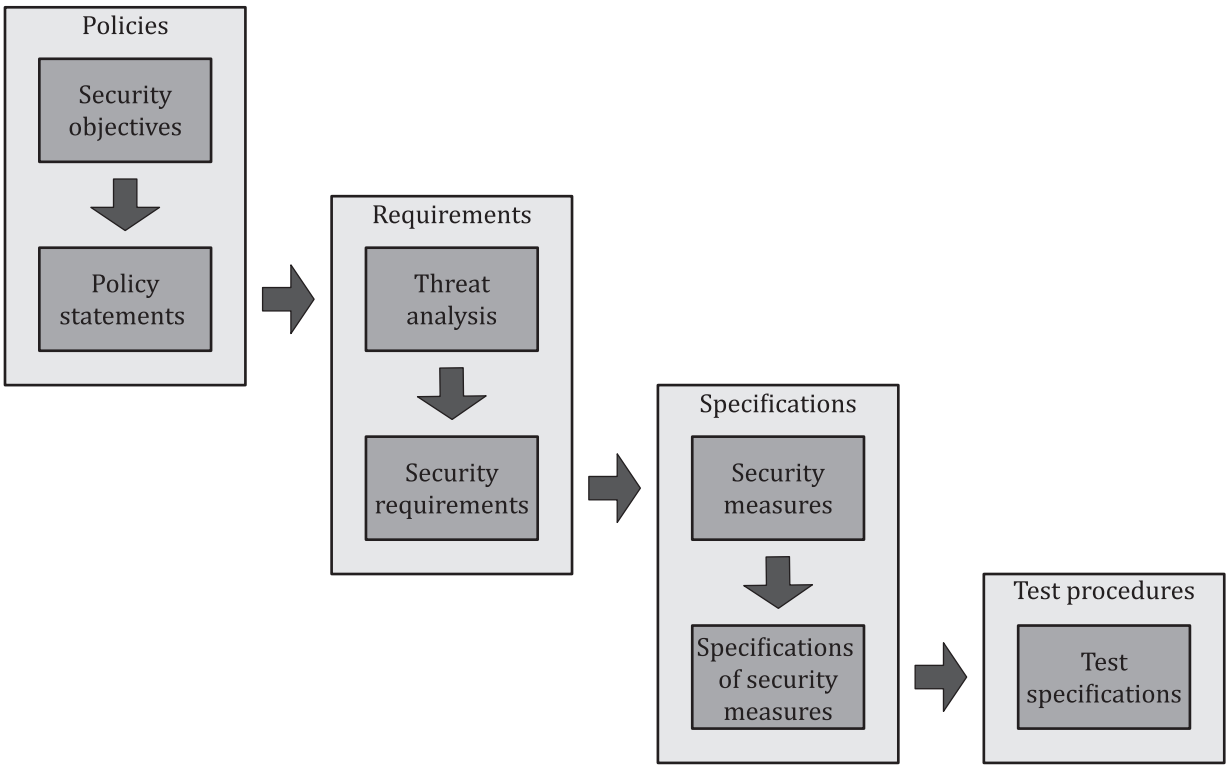

Figure 1 — Development path for the security documents

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.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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 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 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 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

— 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).

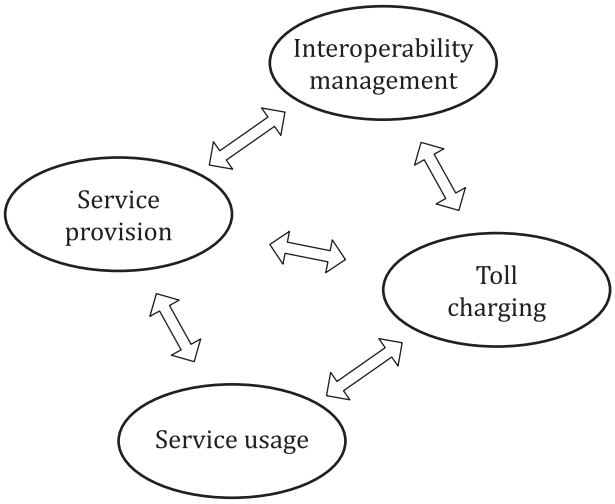

Figure 2 — Role model underlying this document

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.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

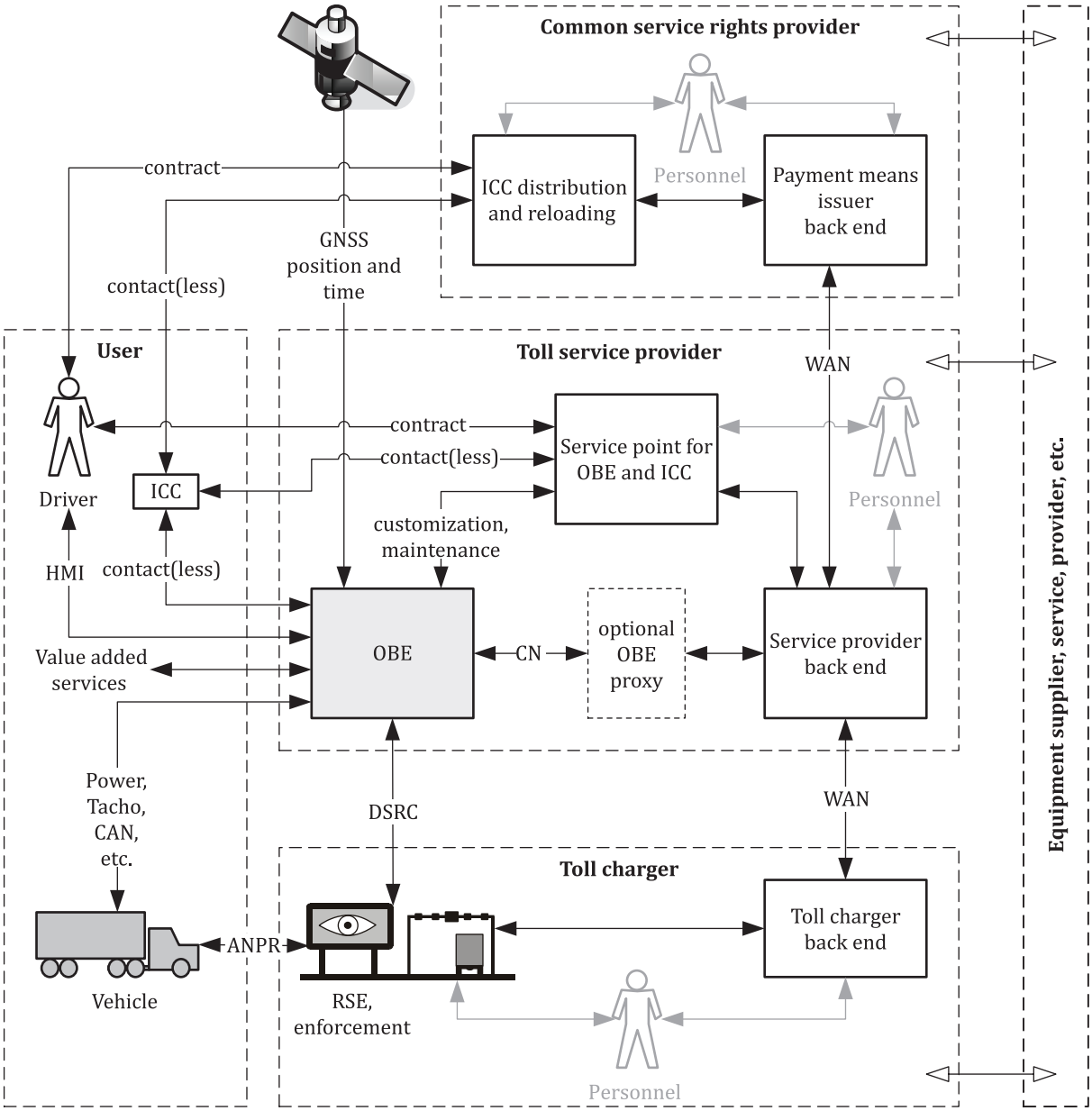

Figure 3 — EFC system model of the EFC security framework

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.

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

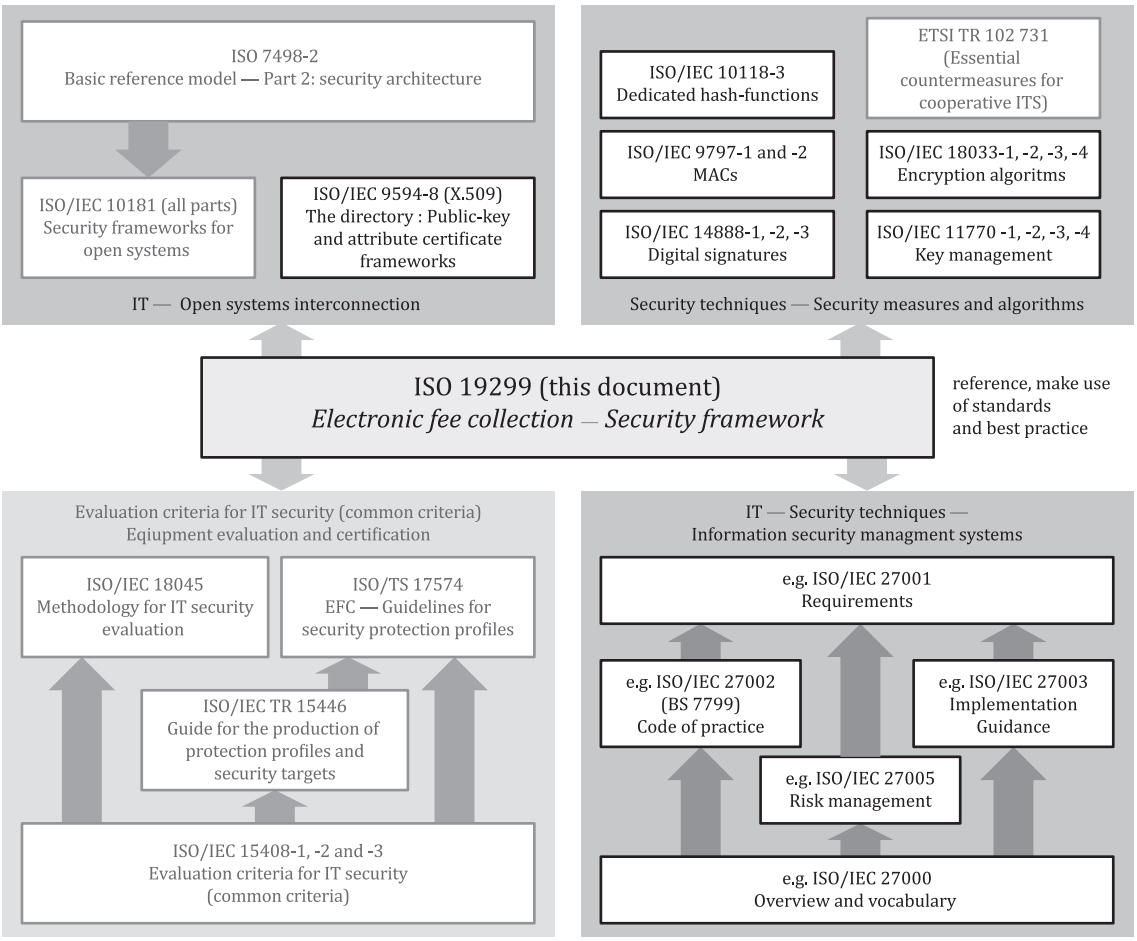

Figure 4 — Relevant security standards in the context of the EFC — Security framework

Standards shown in Figure 4 are grouped in the following categories, where arrows inside each group indicate which standard provides input to other standards:

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

— **IT — Open system interconnection**: provides mechanisms for the secure communications between open systems. These 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)**: defines methodologies and processes for the security evaluation and certification for most categories of products used in the EFC environment.

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

An ISO/IEC 27001 certification of a TC or TSP organization may be used to demonstrate conformity with this document, provided that the scope and the Statements of Applicability (SoA) include the EFC business processes specified in ISO 17573-1 and that security requirements and their associated security measures provided by this document are applied, for example by using them as part of so-called catalogues, i.e., sets containing the security measures and control objectives. Figure 5 illustrates how this approach works in two parallel paths. The first step of both paths is analysing the business

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

processes, which is then followed by a threat analysis. A common risk analysis combines the generic and the EFC related analysis and results in the respective security measures and controls.

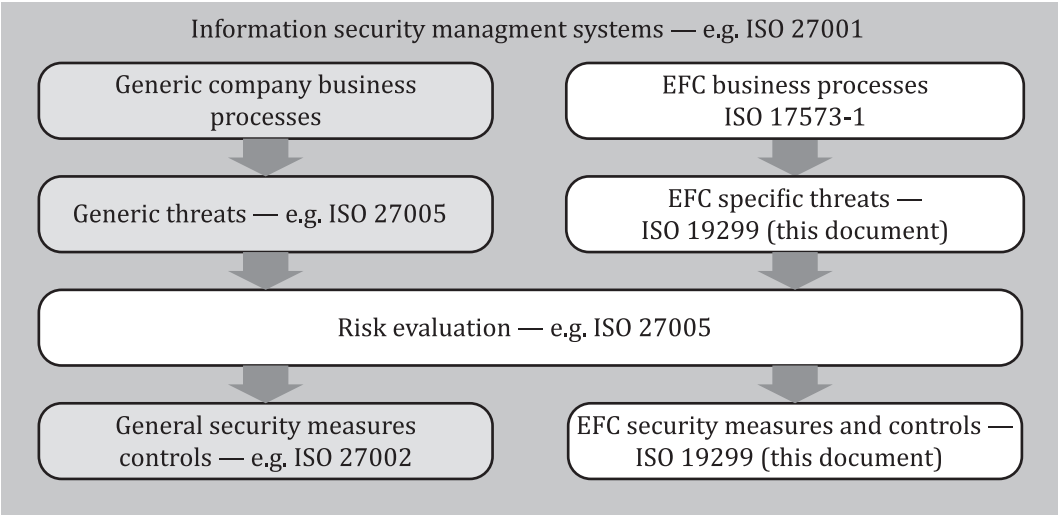

Figure 5 — Scope in relation to the information security management system

In addition, the EFC security framework makes use of existing threat analysis methods and uses existing threat analysis with relation to EFC or ITS, such as ETSI/TR 102 893.

This document contains:

— definition of a trust model (Clause 5): basic assumptions and principles for establishing trust between the stakeholders;

— security requirements (Clause 6): security requirements to support EFC system implementations;

— security measures — countermeasures (Clause 7);

— security specifications for interface implementation (Clause 8): security add-on to EFC standards, as shown in Figure 6;

— key management (Clause 9): initial setup of key exchange between stakeholders and several operational procedures, such as key renewal, certificate revocation;

— security profiles (Annex A);

— implementation conformance statement (Annex B): checklist to be used by an equipment supplier, a system implementation, or an actor of a role declaring their conformity to this document;

— 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).

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

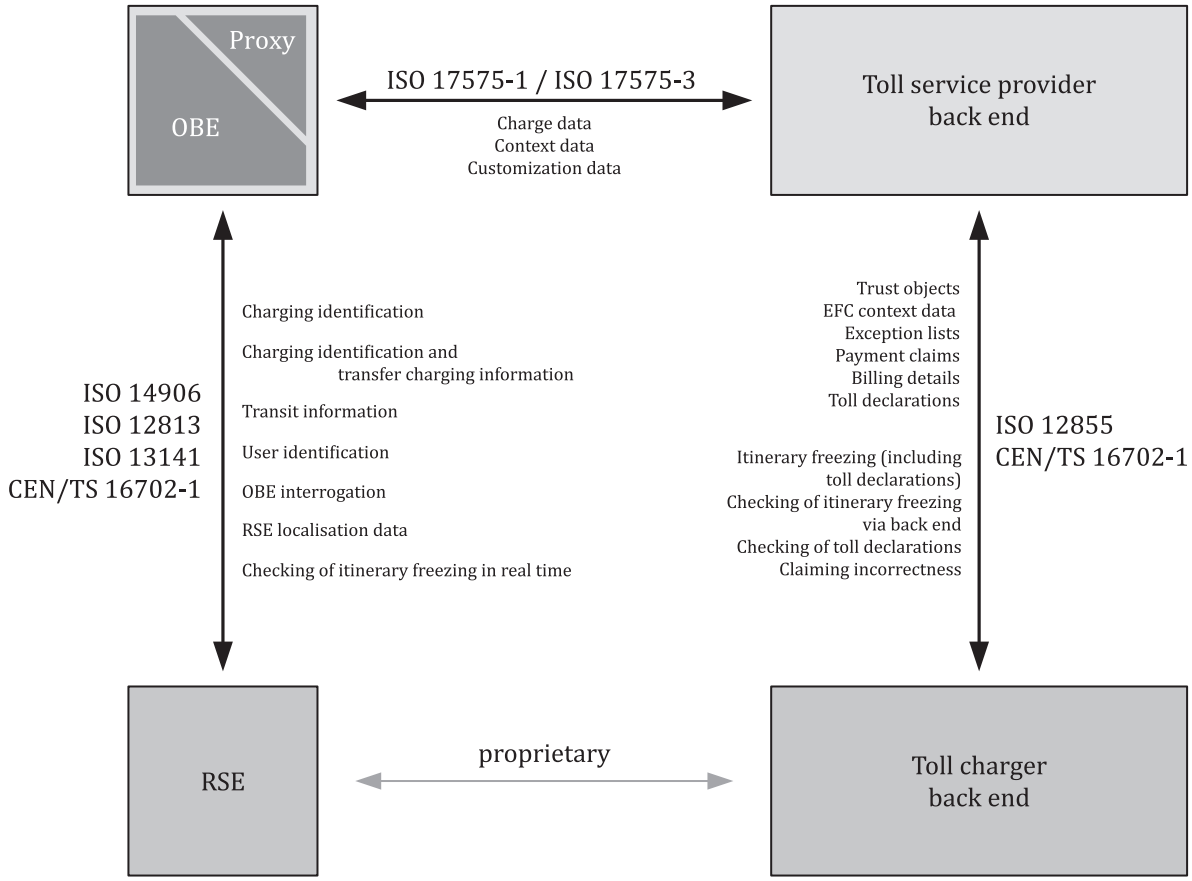

Figure 6 — Scope of EFC security framework for secure communication

This document does not encompass:

— 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.

— the technical trust relation between TSP and service user;

— specifications for implementation of security for specific EFC services, such as 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, for example ICC issued by it.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Electronic fee collection — Security framework

1 Scope

This document defines an information security framework for all organizational and technical entities of an EFC scheme and for the related interfaces, based on the system architecture defined in ISO 17573-1. The security framework describes a set of security requirements and associated security measures.

Annex D contains a list of potential threats to EFC systems and a possible relation to the defined security requirements. These threats can be used for a threat analysis to identify the relevant security requirements for an EFC system.

The relevant security measures to secure EFC systems can then be derived from the identified security requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 2859-1, *Sampling procedures for inspection by attributes — Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection*

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 9594-8:2017, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

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

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

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

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

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

ISO/TS 17573-2, *Electronic fee collection — System architecture for vehicle related tolling— Part 2: Vocabulary*

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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*

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

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

IETF RFC 4648:2006-10, *The Base16, Base32, and Base64 Data Encodings*

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

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 terms and definitions given in ISO/TS 17573-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
asset
anything that has value to a stakeholder

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

[SOURCE: ISO/TS 17573-2:2020, 3.9, modified — Note 1 to entry added.]

3.2
certification authority
CA
entity trusted by one or more entities to assign and revoke public key certificates

[SOURCE: ISO 21188:2018, 3.21]

3.3
data subject's consent
any freely given specific and informed written indication of its wishes by which the data subject signifies its agreement to personal data relating to it being processed

3.4
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.

[SOURCE: ISO/TS 17573-2:2020, 3.73, modified — Note 1 to entry added.]

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

3.5
lot
definite amount of items, delivered together

Note 1 to entry: An inspection lot may consist of several batches or parts of batches.

[SOURCE: ISO 2859-1: 1999, 3.1.13, modified.]

3.6
policy
intentions and direction of an organization, as formally expressed by its management

[SOURCE: ISO/IEC 27000:2018, 3.53, modified.]

3.7
sample
set of one or more items taken from a lot and intended to provide information on the *lot*

[SOURCE: ISO 2859-1: 1999, 3.1.15]

3.8
service user
SU
generic term used for the customer of a toll service provider, one liable for toll, the owner of the vehicle, a fleet operator, a driver, depending on the context

4 Abbreviated terms

AC_CR	access credentials (ISO 14906)
ADU	application data unit
CA	certification authority (ISO 21188)
CCC	compliance check communication (ISO 12813)
CN	cellular network
CRL	certificate revocation list
DSRC	dedicated short-range communication (ISO 14906)
EETS	European electronic toll service
EFC	electronic fee collection (ISO 17573-1)
GNSS	global navigation and satellite system (ISO 17573-1)
HTTP	hypertext transfer protocol
HTTPS	http over secure socket layer
HW	Hardware
ICC	integrated circuit(s) card
ICS	implementation conformance statement (ISO 14907-2) NOTE Under preparation. Stage at the time of publication: ISO/DIS 14907-2:2020.
IETF	internet engineering task force

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

IM	interoperability management
IPsec	internet protocol security
ISMS	information security management system (e.g. ISO/IEC 27001)
LAC	localization augmentation communication (ISO 13141)
MAC	message authentication code
MAC_TC	DSRC message authentication code for toll charger
MAC_TSP	DSRC message authentication code for toll service provider
OBE	on-board equipment (ISO 14906)
OID	object identifier
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)
SAM	secure application module
SHA-1	secure hash algorithm (ISO/IEC 10118-3)
SM	security measure (countermeasure)
SU	service user
SW	software
TC	toll charger (ISO 17573-1)
TLS	transport layer security
TSP	toll service provider
TTP	trusted third party
VPN	virtual private network

5 Trust model

5.1 Overview

The trust model provides the basic trust and functionality for the implementation of authenticated and secured communication channels among toll service provider (TSP), toll charger (TC) and interoperability management (IM).

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

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

The trust model assumes that no initial technical trust relation between any of the stakeholders exists or is provided 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:

— between TC and TSP;

— between TSP and SU;

— between TC or TSP and IM.

There is no direct trust relation between TC 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.

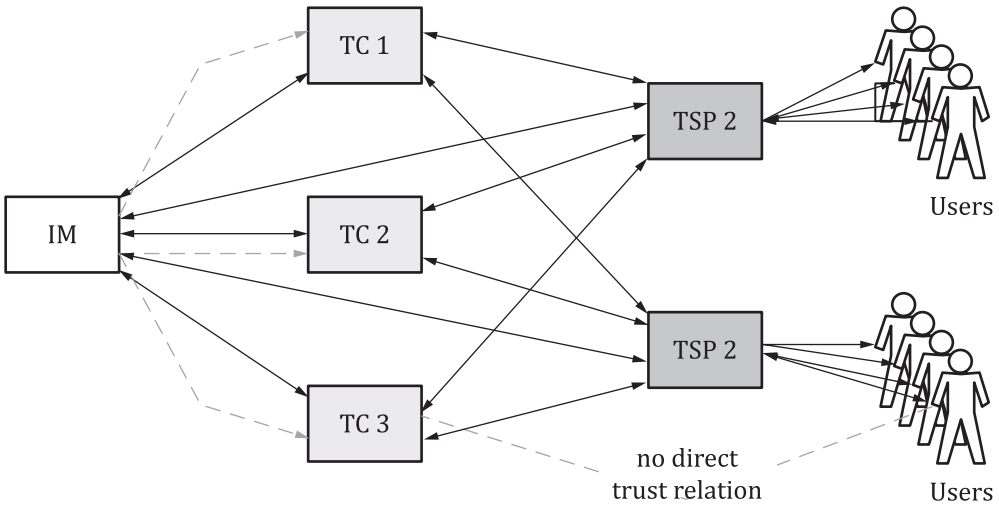

Figure 7 — Stakeholder trust relations

The interoperability management can be a single organization or a set of several entities performing different tasks. Issuing rules, regulations, and general user information by the interoperability management (IM) is performed by means of a trusted relation which is outside of the scope of this document (dotted arrows in Figure 7). Trust relations between IM and TC or TSP 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 relation can include the IM relations to TC and TSP. The TTP may either be performed as a part of the IM, or external TTP(s) may be used to issue the root certificates. This document does not require a mandatory TTP in a hierarchical trust model but supports the use of it.

Another supported model is based on an agreement between TC and TSP (direct trust), which is performed by exchanging self-signed root certificates. Such a peer-to-peer trust relation can also include the IM relations to TC and TSP. This document 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 document.

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

5.3 Technical trust model

5.3.1 General

The technical trust model defines the trust relations between the different stakeholders.

5.3.2 Trust model for TC and TSP relations

The technical trust model uses the Rec. ITU-T X.509 (10/2016)| ISO/IEC 9594-8 version 3 public-key and attribute certificate frameworks for establishing secure communication channels. These secure communication channels 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 the one hand, and a TTP certification authority (CA) approach on the other hand.

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

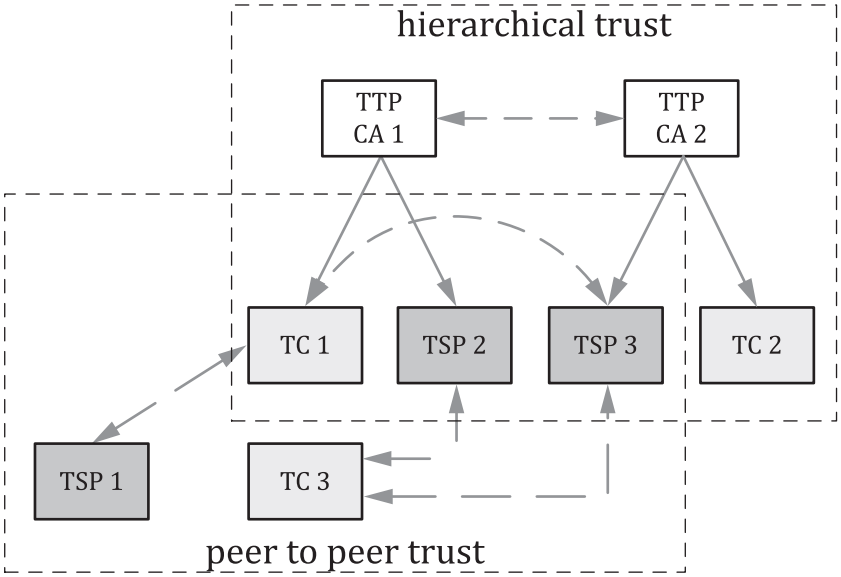

Figure 8 — Example of a mixed trust model environment

Figure 8 indicates the possibility of a trust model allowing an entity to participate in a mixed environment that uses 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. Therefore, there is also a trust relation between TC1 and TSP3.

The dotted box marked as “peer-to-peer trust” shows entities generating self-signed root 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.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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 on 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.

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 17573-1, the operation of the OBE and the provision of toll declarations in a secure way is part of the TSP role. Requirements for achieving end-to-end security from the OBE to the interface to the TCs systems is therefore considered to be an internal interface of the TSP. If security requirements from Clause 6 for end-to-end security are imposed by the security policy, the associated security measures from Clause 7 need to be implemented.

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 methods such as physical mail and face to face meetings. No technical trust model is required for either of these communications.

For all 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 set the technical trust relation.

The initial step for setting up 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 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.

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). Exchange of the root certificates shall be done with one of the following two public key transport mechanisms:

— Mechanism 1: This mechanism shall 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)

© ISO 2020 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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 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 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.

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

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.

For recommended key length and validity periods, see, for example:

— the ENISA recommendations from 2014 under https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

— the NIST recommendations from 2016 under https://www.keylength.com/en/4/ or

— the ECRYPT-CSA recommendations from 2018 under https://www.keylength.com/en/3/.

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

Replacement of a root certificate shall be done as specified 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.

A certificate issuer shall be able to revoke a root certificate before its expiration. Revocation of a root certificate shall be done by a procedure similar to the termination of the commercial contract between TC and TSP and results in a termination of the trust relation. The trust relation shall automatically end when a root certificate is revoked.

Information about revocation of a root certificate shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8, signed with 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 document.

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

The 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 containing 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

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

— message or key encryption purposes.

These end-entity certificates should have a validity period of less than two years.

Information about revocation of an end-entity certificate shall be distributed by 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.

5.4.4 Certificate and certificate revocation list profile and format

The certificates issued according to ISO/IEC 9594-8 certificates version 3 and the CRL according to ISO/IEC 9594-8 version 2 shall conform to the profile defined in IETF RFC 5280 with the update specified in RFC 6818. An implementation compliant to the above documents 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.

5.4.5 Certificate extensions

Considering IETF RFC 5280:2008, 4.2 and clarifications in ISO/IEC 9594-8:2017, 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 system shall reject a 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:

1) key usage: the values in Table 1 shall be used.

2) extended key usage with object identifier (OID) for the following:

   — TC to TSP interface certificate;

   — front end to TSP back end interfaces certificate.

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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

i) CRL distribution points;

ii) authority information access.

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

— basic constraints;

— CRL distribution points;

— authority information access.

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 protect against or to mitigate the threats to an EFC system or to reduce 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 the 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)[8], if applicable;

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

Mainly motivated by the threat analysis in Annex D, the following subclause 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 operator's 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, for example, the ISO/IEC 27000 series.

In order to be compliant with this document, an implementation shall fulfil all requirements selected in accordance with the applicable security policy. Any security measures from Clause 7 that are associated

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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, implementation of the associated security measure is not mandatory. 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 shall be implemented.

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

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 and, if applicable, the associated 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 document 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 other 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. It is recommended to perform this risk analysis according to ISO/IEC 27005, for example.

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). The ISMS shall consider the EFC business processes specified in ISO 17573-1 within its scope and consider, among others, the risks identified in this document. The security measures defined in this document 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 (see Table 3).

Table 3 — ISMS requirements

No.	Requirement	DSRC	GNSS
RQ.ISMS.01	An Information Security Management System (ISMS) shall be established, implemented, operated, maintained, and continuously improved. An ISMS according to ISO/IEC 27001 or equivalent should be used.	X	X
RQ.ISMS.02	Non-EFC specific threats shall be covered by a security measure or security control. Security measures or security controls defined by ISO/IEC 27002 or equivalent should be used.	X	X

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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
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 requirements in Table 5 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.04	The amount of sensitive EFC data stored on an ICC shall be minimized	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

Table 6 lists the requirements for protection of the TCs assets.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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, it 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, it 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
RQ.TC.06	The TC shall make sure that any invoices generated in its name and on its behalf are conformant to the invoicing rules of its country (enabled by RQ.TSP.56).	X	X
RQ.TC.07	The TC shall ensure that the TSPs OBE is suitable for use in its toll domain.	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 set of keys for OBE communication provided by the TSP.	X	X
RQ.TC.11	The TC shall implement all necessary technical and organizational mechanisms for a correct implementation of a set of keys for ICC communication provided by the ICC issuer.	X	X
RQ.TC.12	The TC shall make sure that its 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 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 TC shall not allow unauthorized access to RSE software and data.	X	X
RQ.TC.25	The TC shall guarantee confidentiality, integrity and non-repudiation with proof of origin of a set of keys for OBE communication during transfer to the RSE.	X	X
RQ.TC.26	The TC shall guarantee confidentiality, integrity and non-repudiation with proof of origin of a set of keys for ICC 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

© ISO 2020 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 6 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TC.50	A data protection commissioner or delegate shall have the possibility to audit the system for compliance with data privacy regulations. Such audits shall be used to prove the data protection concept.	X	X
RQ.TC.51	The TC shall publish its procedures of collecting and processing personal data or register them 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
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 its back office interfaces according to agreed service levels.	X	X
RQ.TC.96	The TC shall be responsible for the availability of its 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

Table 7 lists the requirements for the protection of the TSP's 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

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 7 *(continued)*

No.	Requirement	DSRC	GNSS
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	n.a.
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.15	The ICC shall not allow the service user to modify fixed account data.	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 duplicate or false 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 shall be in compliance with the privacy requirements of the toll domain.	X	X
RQ.TSP.43	The TSP shall store entry evidence data of a vehicle in the data group ReceiptEntryVehicle (see ISO/TS 21193) inside an ICC in a closed toll regime.	X	X
RQ.TSP.44	The TSP shall verify the entry evidence data stored in the data group ReceiptEntryVehicle (see ISO/TS 21193) inside an ICC with the current vehicle information on an exit transaction in a closed toll regime.	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 its 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

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 7 *(continued)*

No.	Requirement	DSRC	GNSS
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 its procedures of collecting and processing personal data or register them 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 extensively test all features of an OBE update before it is implemented (e.g. distributed over the air).	X	X
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 shall 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	Initialisation and 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.95	The TSP shall be responsible for the availability of its back office interfaces according to agreed service levels.	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 to guarantee 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 (see Table 8).

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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 requirements in Table 9 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 feasible because it is much too expensive. The requirements in Table 9 are not further treated in this document.

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 hardware (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 document, 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.

Table 10 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.

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

7.2 General security measures

This document 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. These 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 (see Table 11).

Table 11 — General security measures

No.	Security measure	DSRC	GNSS
		Fulfilled RQ	
SM.101	The TC and TSP shall publish their procedures of collecting and processing personal data or 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.91	
SM.102	The TC and the TSP shall sign an agreement on the protection of personal data 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.91 RQ.TC.06 RQ.TSP.56 RQ.TSP.89	
SM.103	The contracting parties of communication providers shall sign an agreement on the protection of personal data 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.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 agreement on the protection of personal data.	X	X
		RQ.TSP.42 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 agreement on the protection of personal data.	X	X
		RQ.TSP.42 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 its name. The TC shall periodically audit invoices to service users for tolls of its toll domain.	X	X
		RQ.TC.06 RQ.TSP.56 RQ.TSP.89	

7.3 Communication interfaces security measures

7.3.1 General

Table 12 contains the security measures for the protection of data exchanged between entities using the different interfaces.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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	
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 RQ.TSP.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 RQ.TSP.90	
SM.203	Security measures or security controls shall be implemented. Security measures or security controls defined by ISO/IEC 27002 or equivalent should be used.	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.95 RQ.TSP.96	
SM.205	An information security management system (ISMS) shall be implemented. An ISMS according to ISO/IEC 27001 or equivalent should be used.	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 lists the security measures for protection of the DSRC-EFC interface.

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

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	
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.TC.04 RQ.TC.05 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	
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 lists the security measures for protection of the 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	

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 14 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
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 Payment-Means 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	
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 lists the security measures for protection of the 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 lists the security measures for protection of the 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.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 2020 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS EN ISO 19299:2020

7.3.6 TC to TSP interface

Table 17 lists the security measures for protection of the 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 it.	X	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12	
SM.252	If the TSP receives billing details from the TC, it 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 its 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 it to calculate the amount given in the billing details. NOTE Other means than the interface defined in ISO 12855 can be used, such as publication on a website.	X	X
		RQ.TC.98 RQ.TSP.12	

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 17 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.259	The TSP shall perform plausibility and completeness checks on received billing details. NOTE Those checks can 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 it.	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.92	
SM.264	The TC shall guarantee the correct manual entry or automatic processing of a set of keys 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	
SM.267	The TC shall guarantee the correct manual entry or automatic processing of a set of keys for ICC communication provided by the ICC issuer.	X	X
		RQ.TC.11 RQ.TC.26	

7.3.7 ICC interface

Table 18 lists the security measures for protection of the ICC interface.

Table 18 — ICC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.270	The ICC shall request the OBE to calculate and provide an authentication code complying with ISO/IEC 7816-3 command/response using a key known only to the ICC issuer, if sensitive EFC data is stored inside an ICC.	X	X
		RQ.IF.11 RQ.IF.12	
SM.271	The ICC shall use cryptographic measures to encrypt any sensitive EFC data stored on the ICC to guarantee data integrity and non-repudiation with proof of origin, if sensitive EFC data is stored inside an ICC.	X	X
		RQ.IF.11 RQ.DS.05 RQ.DS.06	
SM.272	Entry evidence data of a vehicle shall be stored in the data group ReceiptEntryVehicle (see ISO/TS 21193) inside an ICC, if this data group is provided by the ICC.	X	X
		RQ.TSP.43	
SM.273	The amount of sensitive EFC data stored on the ICC shall be minimized to provide for data protection regulations.	X	X
		RQ.DS.04 RQ.TSP.59	

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 18 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.274	The RSE shall verify the recorded exit evidence data of a vehicle with the entry evidence data, if entry evidence data is stored in the data group ReceiptEntryVehicle (see ISO/TS 21193) inside an ICC.	X	X
		RQ.TSP.44	
SM.275	The TC shall check the validity of the ICC to ensure a valid payment guarantee of the TSP for the existing service user.	X	X
		RQ.TC.93	
SM.276	The TC shall support the exchange of keys stored inside the RSE/OBE by the ICC issuer, if sensitive EFC data is stored inside an ICC.	X	n.a.
		RQ.TC 11 RQ.TC.26	

7.4 End-to-end security measures

Table 19 lists the security measures for protection of the end-to-end interfaces.

End-to-end security cover the interface from the front end to the TSP to the TC.

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 a 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 their behalf. NOTE An audit process can, for example, compare charge data of sample vehicles equipped with OBE with known independent trip data or monitor the performance of all OBE to identify a bad performing single OBE or batch of OBE.	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 its 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 fallback 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	

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 19 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
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 its 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	
SM.323	The TSP shall perform plausibility and completeness checks on toll declarations acquired by it. 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 fallback 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 lists the security measures for protection of the front end/OBE interface.

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 when it passes such an 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 statistically significant sample out of a lot of OBE delivered to it by the OBE manufacturer to achieve an accepted quality level according to ISO 2859-1 or equivalent.	X	X
		RQ.TSP.80	

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 20 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
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.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	
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 except the data allowed to be changed through the user interface.	X	X
		RQ.TSP.06 RQ.TSP.15	

7.5.2 Back end security measures

Table 21 lists the security measures for protection of the TSP back end interface.

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.21	
SM.422	The TSP shall verify the integrity of the charge report.	n.a.	X
		RQ.TSP.01	

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 21 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.423	The TSP shall include stolen or cloned OBE or ICC in an exception list.	X	X
		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.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 OBE manufacturer shall use cryptographic measures to encrypt the sending of initialization data to the OBE to guarantee data integrity and non-repudiation with proof of origin.	X	X
		RQ.TSP.92 RQ.TSP.97	
SM.427	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	

7.6 Toll charger security measures

7.6.1 RSE security measures

Table 22 lists the security measures for protection of the RSE interface.

Table 22 — RSE security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.510	If toll declarations are acquired through the DSRC interface, the TC shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TC.04 RQ.TC.05	
SM.511	If toll declarations are acquired through the DSRC interface, the TC shall store the value of the transaction counter read-out of the OBE as part of the billing details.	X	n.a.
		RQ.TSP.21	
SM.512	If toll declarations are acquired through the DSRC interface, the TC shall store the value of the authenticated AttributeList, MAC_TSP, KeyRef and RndRSE as part of the billing details.	X	n.a.
		RQ.IF.12 RQ.IF.13	
SM.513	If toll declarations are acquired by the TSP, the dedicated compliance checking RSE of the TC shall perform a Compliance Checking Communication transaction over an interface with security as defined in ISO 12813 when an OBE passes it or use secure monitoring-compliance checking.	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TC.05 RQ.TSP.53	

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 22 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.514	If compliance checking is performed through the DSRC interface, the TC shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TC.04	
SM.515	If compliance checking is performed through the DSRC interface, the TC shall store the value of the authenticated AttributeList, MAC_TC, MAC_TSP, KeyRef and RndRSE as part of the compliance check record.	n.a.	X
		RQ.IF.12 RQ.IF.13	
SM.516	The RSE's functionality shall be tested to guarantee its functionality.	X	X
		RQ.TC.70	

7.6.2 Back end security measures

Table 23 lists the security measures for protection of the TC back end interface.

Table 23 — TC Back end security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.520	The TC shall perform plausibility and completeness checks on toll declarations acquired by it through the DSRC interface.	X	n.a.
		RQ.TC.12	
SM.521	If toll declarations are acquired by the TSP and these are based on LAC data, the TC shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.04 RQ.TC.05	
SM.522	The TC shall check the exception list to ensure a valid payment guarantee of the TSP for the existing service user.	X	X
		RQ.TC.92 RQ.TC.93	
SM.523	The TC shall use cryptographic measures to guarantee confidentiality, data integrity and non-repudiation with proof of origin of a set of keys for OBE communication during transfer to the RSE.	X	X
		RQ.TC.25	
SM.524	The TC shall make sure that all relevant toll declarations are considered before initiating enforcement procedures against a service user.	X	X
		RQ.TC.30	
SM.525	The TC shall use cryptographic measures to guarantee data integrity and non-repudiation with proof of origin for all recorded data regarding an enforcement case.	X	X
		RQ.TC.32	

7.6.3 Other TC security measures

Table 24 lists other TC security measures that are not covered in the previous tables.

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

Table 24 — Other TC security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.530	If toll declarations are acquired through the DSRC interface, the TC shall compare them with its own observations in accordance with privacy regulations.	X	n.a.
		RQ.TC.01	

8 Security specifications for interoperable interface implementation

8.1 General

8.1.1 Subject

This subclause defines the detailed documents supplementing the definitions in other standards that shall be implemented to fulfil those security measures defined in Clause 7 that are directly related to an application data unit (ADU) specification of an interoperable interface.

8.1.2 Signature and hash algorithms

The signature and hash algorithms for proof of message authenticity, integrity, and non-repudiation shall be implemented according to the following standards:

— security specifications for TC to TSP back office interface: ISO 12855;

— security specifications for front end to TSP interface: ISO 17575-1;

— non-DSRC MAC algorithm: CEN/TS 16702-1;

— security specifications for CCC: ISO 12813;

— security specifications for LAC: ISO 13141.

8.2 Security specifications for DSRC-EFC

8.2.1 Subject

This subclause provides the implementation of security measures SM.210, SM.211, SM.212, SM.214, and SM215.

8.2.2 OBE

The OBE shall comply with the security measures of EN 15509:2014 security level 1 or equivalent standard.

8.2.3 RSE

The RSE shall comply with the security measures of EN 15509:2014 security level 1 or equivalent standard. The RSE may additionally support OBE that comply with EN 15509:2014 security level 0 or equivalent standards.

NOTE Security level 0 will provide compatibility with legacy OBE not supported by this document.

The RSE shall request MAC_TC and MAC_TSP by addressing at least the PaymentMeans attribute.

The exact values of KeyRef to be used shall be subject of agreement between TC and TSP.

© ISO 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020

9 Key management

9.1 Overview

Keys are a critical part of any security system that relies on cryptographic techniques. The appropriate protection of keys depends on a number of factors such as the type of application for which the keys are used, the threats they face, the different states the keys may assume, etc. Primarily, depending upon the cryptographic technique, they should protected against disclosure, modification, destruction and replay.

NOTE ISO/IEC 11770-1:2010, Annex A provides a list of threats to key management.

The objective of key management is the secure administration and use of key management services and therefore, the protection of keys is extremely important. Key management procedures depend on the underlying cryptographic mechanisms, the intended use of the key, and the security policy in use. Key management also includes those functions that are executed in cryptographic devices.

Key management is the administration and use of the services of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of keying material.

9.2 Asymmetric keys

9.2.1 Key exchange between stakeholders

The exchange of root public keys, i.e. CA root certificates, is defined in 5.4.1.

The exchange of entity public keys, i.e. end-entity certificates, shall be according to the public key transport mechanism 3 defined in ISO/IEC 11770-3.

In the case of public key transport mechanism 3, the certificate verification procedure shall include the check of the certificate attribute “Extended Key Usage” with OID for the following:

— TC to TSP interface certificate;

— Front End to TSP Back End interfaces certificate.

9.2.2 Key generation and certification

Key generation and certification including certificate life cycle management (including, among others, key generation and certification processes) shall be performed at least according to ISO/IEC 11770-1:2010, Annex D.

Random bit generators (e.g. for the generation of session keys) shall comply with the requirements defined in ISO/IEC 18031.

NOTE Additional information and guidance for asymmetric key management and PKIs is provided for example in reference [30].

9.2.3 Protection of keys

Private keys for ADU authentication and/or decryption shall be stored in a cryptographic module designed according to one of the following example security standards and protection profiles:

— ISO/IEC 19790 (minimum level 3);

— FIPS PUB 140-2 (minimum security level 3);

— common criteria protection profile BSI-PP-0002 (minimum EAL4).

© ISO 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 19299:2020