

SLOVENSKI STANDARD

SIST EN ISO 17574:2026

01-november-2026

Nadomešča:

SIST-TS CEN ISO/TS 17574:2017

Elektronsko pobiranje pristojbin - Zahteve za zaščito varnostnih profilov EFC (ISO 17574:2026)

Electronic fee collection - Requirements for security protection profiles (ISO 17574:2026)

Elektronische Gebührenerhebung - Leitfaden für Sicherheitsprofile (ISO 17574:2026)

Perception de télépéage - Exigences relatives aux profils de protection de sécurité (ISO 17574:2026)

Ta slovenski standard je istoveten z: EN ISO 17574:2026

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST EN ISO 17574:2026

en,fr,de

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 17574

September 2026

ICS 03.220.20; 35.240.60

Supersedes CEN ISO/TS 17574:2017

English Version

**Electronic fee collection - Requirements for security
protection profiles (ISO 17574:2026)**

Perception de télépéage - Exigences relatives aux
profils de protection de sécurité (ISO 17574:2026)

Elektronische Gebührenerhebung - Leitfaden für
Sicherheitsprofile (ISO 17574:2026)

This European Standard was approved by CEN on 27 July 2026.

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, Türkiye and United Kingdom.

get full document from standards.iteh.ai



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

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

© 2026 CEN All rights of exploitation in any form and by any means reserved
worldwide for CEN national Members.

Ref. No. EN ISO 17574:2026 E

Contents	Page
European foreword.....	3

Sample Document

get full document from standards.iteh.ai

European foreword

This document (EN ISO 17574:2026) 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 2027, and conflicting national standards shall be withdrawn at the latest by March 2027.

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 17574:2017.

This document has been prepared under a standardization request addressed to CEN by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

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, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO 17574:2026 has been approved by CEN as EN ISO 17574:2026 without any modification.

Sample Document

get full document from standards.iteh.ai



**International
Standard**

ISO 17574

**Electronic fee collection —
Requirements for security
protection profiles**

*Perception de télépéage — Exigences relatives aux profils de
protection de sécurité*

**First edition
2026-09**

Sample Document

get full document from standards.iteh.ai

ISO 17574:2026(en)

Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

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

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2026 – All rights reserved

ISO 17574:2026(en)

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 EFC security architecture and protection profile processes	2
5.1 General	2
5.2 EFC security architecture	3
5.3 Protection profile preparatory steps	3
5.4 Relationship between actors	4
6 Outline of protection profile (PP)	6
6.1 Structure	6
6.2 Context	6
Annex A (informative) Procedure to prepare the protection profile	8
Annex B (informative) Example of threat analysis evaluation method	40
Annex C (informative) Relevant security standards in the context of the EFC	46
Bibliography	47

Sample Document

get full document from standards.iteh.ai

ISO 17574:2026(en)

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 document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 the third edition (ISO/TS 17574:2017), which has been technically revised.

The main changes are as follows:

- [Clause 3](#) has been updated and ISO 17573-2 has been made the primary source for terms and definitions;
- requirements have been updated to reflect the latest edition of the ISO/IEC 15408 series.

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 17574:2026(en)

Introduction

Electronic fee collection (EFC) systems are subject to several ways of fraud both by users and operators but also from people outside the system. These security threats are countered with various types of security measures linked to specified security requirements.

It is recommended that EFC operators prepare their own EFC protection profile (PP) according to this document, as security requirements should be described from the operator's point of view.

A protection profile (PP) refers to a set of safety requirements for a category of products or systems that meet specific needs. A typical example is a PP for on-board equipment (OBE) to be used in an EFC system. However, the requirements in this document are superseded if a PP already exists for the subsystem in question.

The target of evaluation (TOE) for EFC is limited to EFC specific roles and interfaces as shown in [Figure 1](#). [Figure 1](#) shows the relationships and interactions among the entities related to the TOE of the EFC. As shown in this figure, entities are overall management of the toll charging environment, EFC service provider, toll charger and user of the service. Since the existing financial security standards and criteria are applicable to other external roles and interfaces, they are assumed to be outside the scope of TOE for EFC.

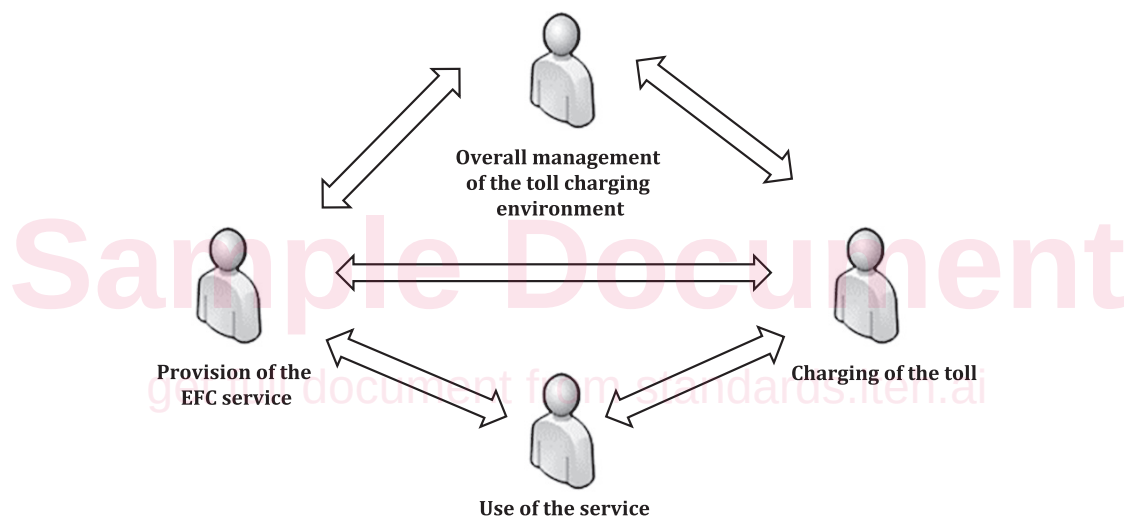


Figure 1 — Scope of TOE for EFC

The security evaluation is performed by assessing the security-related properties of roles, entities and interfaces defined in security targets (STs), as opposed to assessing complete processes which often are distributed over more entities and interfaces than those covered by the TOE of this document.

NOTE Assessing security issues for complete processes is a complementary approach, which can be beneficial to apply when evaluating the security of a system.

It should be noted that the requirements provided in this document are intended to be read in conjunction with the ISO/IEC 15408 series. [Annex A](#) provides an example of how to prepare the security requirements for EFC equipment, in this case, a dedicated short-range communication (DSRC)-based OBE with an integrated circuit(s) card (ICC) containing data needed for the EFC. The example refers to a Japanese national EFC system and should only be regarded as an example.

After an PP for EFC is prepared, it can be internationally registered by the organization that prepared the PP for EFC so that other operators or countries that want to develop their EFC system security services can refer to an already registered PP for EFC.

This document on security service framework and PP for EFC is based on the ISO/IEC 15408 series. The ISO/IEC 15408 series includes a set of requirements for the security functions and assurance of IT-relevant products and systems. Operators, organizations or authorities defining their own PP for EFC can use these

ISO 17574:2026(en)

requirements. The different PPs for EFC defined by operators, organizations or authorities will be similar to the different PPs registered by several financial institutions, e.g. for payment instruments like IC cards (ICCs).

The products and systems that were developed in accordance with the ISO/IEC 15408 series can be publicly assured by the authentication of the government or designated private evaluation agencies.

Sample Document

get full document from standards.iteh.ai

Electronic fee collection — Requirements for security protection profiles

1 Scope

This document specifies electronic fee collection (EFC) requirements for the preparation and evaluation of security requirements specifications, referred to as protection profiles (PP) in the ISO/IEC 15408 series and in ISO/IEC TR 15446.

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/IEC 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 15408-4:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17573-2 apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

ISO 17574:2026(en)

4 Abbreviated terms

CC	common criteria
CCRA	common criteria recognition arrangement
CN	cellular networks
DSRC	dedicated short-range communication
EAL	evaluation assurance level
EFC	electronic fee collection
GNSS	global navigation satellite systems
HMI	human-machine interface
ICC	integrated circuit(s) card
IT	information technology
OBE	on-board equipment
PP	protection profile
RSE	roadside equipment
SAM	secure application module
SFP	security function policy
SFR	security functional requirement
ST	security target
TOE	target of evaluation
TSF	target of evaluation security functions

5 EFC security architecture and protection profile processes**5.1 General**

This clause gives an overview of the context and use of this document in terms of the EFC security architecture and protection profile processes.

This document is intended to be read in conjunction with the ISO/IEC 15408 series and ISO/IEC TR 15446. Although a reader unfamiliar with the standards can read the first part of the document to have an overview on how to prepare a PP for EFC equipment, the annexes, in particular Annexes [A.4](#) and [A.5](#), require the reader to be familiar with the ISO/IEC 15408 series. This document uses an OBE with an integrated circuit(s) card (ICC) as an example to describe both the structure of the PP, as well as the proposed content.

In [Annex A](#), the procedure for preparing PP for EFC is illustrated, which is described by using an OBE as an example of EFC equipment. The communication link (between the OBE and the RSE) is based on DSRC.

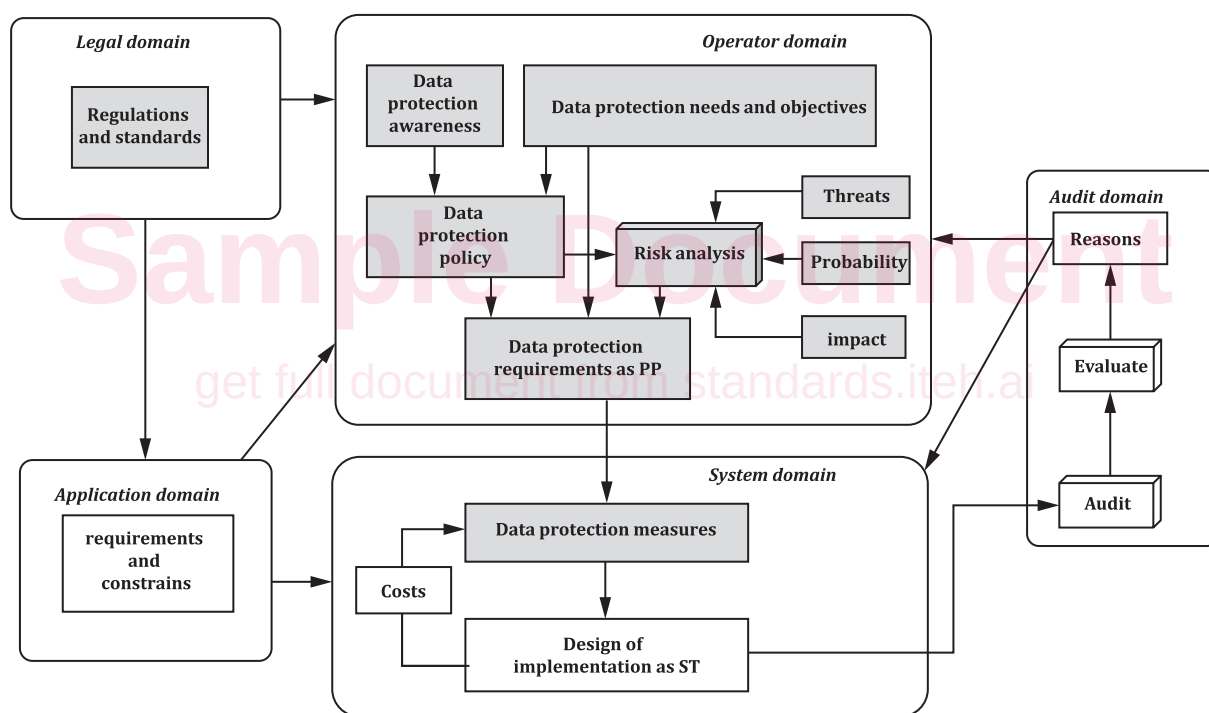
[Annex B](#) gives an example of how a threat analysis can be done, while [Annex C](#) provides an overview of the relevant security standards in the context of the EFC, which provides the background of EFC roles and interfaces.

5.2 EFC security architecture

[Figure 2](#) illustrates the position of this document within the broader context of the EFC security architecture, highlighting the relationships between related domains and information dependencies. The shaded boxes are the aspects mostly related to the preparation of PPs for EFC systems.

Regarding the security design framework, there are five domains. Functionality of these domains are described as below.

- Operator domain defines the data protection requirement of the TOE as PP.
- System domain develops the ST based on the requirement. For development of the ST, threat and risk assessment are done with balancing the cost and effect of the security measures.
- Legal domain defines the relevant regulations and standards.
- Application domain defines the requirement and constraints of the TOE.
- Audit domain conducts the audit and evaluation of validities of design of implementation for data protection measures. As the feedback of the audit and evaluation, reasons are reported to System domain and Operator domain.



Key

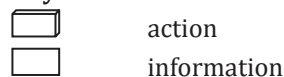


Figure 2 — Overall view of security design framework

5.3 Protection profile preparatory steps

The main purpose of a PP is to analyse the security environment of a subject and then to specify the requirements for each of the threats identified by the security environment analysis. The subject studied is called the target of evaluation (TOE). In this document, an OBE with an ICC is used as an example of the TOE.

The preparatory work of PP for EFC consists of the steps shown in [Table 1](#), according to the contents described in [Clause 6](#).