



SLOVENSKI STANDARD SIST EN ISO 24534-4:2010

01-oktober-2010

Nadomešča:

SIST-TS CEN ISO/TS 24534-4:2008

Avtomatična identifikacija vozil in opreme - Elektronska identifikacija registracije (ERI) za vozila - 4. del: Varne komunikacije, pri katerih se uporabljajo asimetrične tehnike (ISO 24534-4:2010)

Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques (ISO 24534-4:2010)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 24534-4:2010](http://standards.iteh.ai/catalog/standards/sist/175703/isc-129113/72113646/sist-en-iso-24534-4-2010)

Identification automatique des véhicules et des équipements - Identification d'enregistrement électronique (ERI) pour les véhicules - Partie 4: Communications sûres utilisant des techniques asymétriques (ISO 24534-4:2010)

Ta slovenski standard je istoveten z: EN ISO 24534-4:2010

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

SIST EN ISO 24534-4:2010

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 24534-4:2010

<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 24534-4

July 2010

ICS 35.240.60; 03.220.20

Supersedes CEN ISO/TS 24534-4:2008

English Version

**Automatic vehicle and equipment identification - Electronic
Registration Identification (ERI) for vehicles - Part 4: Secure
communications using asymmetrical techniques (ISO 24534-
4:2010)**

Identification automatique des véhicules et des
équipements - Identification d'enregistrement électronique
(ERI) pour les véhicules - Partie 4: Communications sûres
utilisant des techniques asymétriques (ISO 24534-4:2010)

This European Standard was approved by CEN on 16 June 2010.

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 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 Management Centre has the same status as the official versions.

[SIST EN ISO 24534-4:2010](https://standards.iteh.ai/standards/iso/24534-4/2010)

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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword.....3

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

[SIST EN ISO 24534-4:2010](https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010)

<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>

Foreword

This document (EN ISO 24534-4:2010) has been prepared by Technical Committee CEN/TC 278 "Road transport and traffic telematics", the secretariat of which is held by NEN, in collaboration with Technical Committee ISO/TC 204 "Intelligent transport systems".

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 January 2011, and conflicting national standards shall be withdrawn at the latest by January 2011.

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

This document supersedes CEN ISO/TS 24534-4:2008.

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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

iTeh STANDARD PREVIEW (standards.iteh.ai)

Endorsement notice

The text of ISO 24534-4:2010 has been approved by CEN as a EN ISO 24534-4:2010 without any modification.

[SIST EN ISO 24534-4:2010
https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010](https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 24534-4:2010

<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>

INTERNATIONAL
STANDARD

ISO
24534-4

First edition
2010-07-15

**Automatic vehicle and equipment
identification — Electronic registration
identification (ERI) for vehicles —**

**Part 4:
Secure communications using
asymmetrical techniques**

iTeh STANDARD PREVIEW

(standards.iteh.ai)
*Identification automatique des véhicules et des équipements —
Identification d'enregistrement électronique (ERI) pour les véhicules —*

Partie 4: Communications sûres utilisant des techniques asymétriques

<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>



Reference number
ISO 24534-4:2010(E)

© ISO 2010

ISO 24534-4:2010(E)**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN ISO 24534-4:2010](https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010)

<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>

**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Abbreviations.....	10
5 System communications concept	11
5.1 Introduction.....	11
5.2 Overview.....	11
5.3 Security services	18
5.4 Communication architecture description	23
5.5 Interfaces.....	25
6 Interface requirements.....	26
6.1 Overview.....	26
6.2 Abstract transaction definitions	27
6.3 The ERT interfaces	63
Annex A (normative) ASN.1 modules	66
Annex B (normative) PICS pro forma	77
Annex C (informative) Operational scenarios.....	81
Bibliography.....	93

ISO 24534-4:2010(E)

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 24534-4 was prepared by the European Committee for Standardization (CEN) Technical Committee CEN/TC 278, *Road transport and traffic telematics*, in collaboration with Technical Committee ISO/TC 204, *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO 24534-4 cancels and replaces ISO/TS 24534-4:2008, which has been technically revised.

SIST EN ISO 24534-4:2010

ISO 24534 consists of the following parts, under the general title *Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles*:

- *Part 1: Architecture*
- *Part 2: Operational requirements*
- *Part 3: Vehicle data*
- *Part 4: Secure communications using asymmetrical techniques*
- *Part 5: Secure communications using symmetrical techniques*

Introduction

A quickly emerging need has been identified with administrations to improve the unique identification of vehicles for a variety of services. Situations are already occurring where manufacturers intend to fit lifetime tags to vehicles. Various governments are considering the needs and benefits of electronic registration identification (ERI) as a legal proof of vehicle identity with potential mandatory uses. There is commercial and economic justification in respect of both tags and infrastructure that a standard enables an interoperable solution.

ERI is a means of uniquely identifying road vehicles. The application of ERI will offer significant benefits over existing techniques for vehicle identification. It will be a suitable tool for the future management and administration of traffic and transport, including applications in free-flow, multi-lane traffic conditions with the capability to support mobile transactions. ERI addresses the need of authorities and other road users for a trusted electronic identification, including roaming vehicles.

This part of ISO 24534 specifies the application layer interfaces for the exchange of data between an onboard component containing the ERI data and a reader or writer inside or outside the vehicle.

The exchanged identification data consists of a unique vehicle identifier and may also include data typically found in the vehicle's registration certificate. The authenticity of the exchanged vehicle data can be further enhanced by ensuring data has been obtained by request from a commissioned device, with the data electronically signed by the registration authority.

In order to facilitate (international) resales of vehicles, the ERI interface includes provisions for another accredited registration authority to take over the registration of a vehicle.

The ERI interface supports confidentiality measures to adhere to (inter)national privacy regulation and to prevent other misuse of electronic identification of vehicles. A registration authority may authorize other authorities to access the vehicle's data. A holder of a registration certificate may authorize an additional service provider to identify the vehicle when he/she wants commercial service.

However, it is perceived that different users may have different requirements for authentication and confidentiality. This International Standard therefore supports different levels of security with maximum compatibility. Much attention is given to the interoperability of the component containing the ERI data and readers of various levels of capability, e.g. the identification of a vehicle with a less capable ERI data component by a more sophisticated reader equipment and vice versa.

The supported complexity of the device containing the ERI data may range from a very simple read-only device that only contains the vehicle's identifier, to a sophisticated device that includes both authentication and confidentiality measures and maintains a historic list of the vehicle data written by the manufacturer and by vehicle registration authorities.

Following the events of 11 September 2001, and subsequent reviews of anti-terrorism measures, the need for ERI has been identified as a possible anti-terrorism measure. The need for international or pan-European harmonization of such ERI is therefore important. It is also important to ensure that any ERI measures contain protection against misuse by terrorists.

This part of ISO 24534 makes use of the basic automatic vehicle identification (AVI) provisions already defined in ISO 14814 and ISO 14816.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 24534-4:2010

<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>

Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles —

Part 4: Secure communications using asymmetrical techniques

1 Scope

This part of ISO 24534 provides requirements for electronic registration identification (ERI) that are based on an identifier assigned to a vehicle (e.g. for recognition by national authorities) suitable to be used for:

- electronic identification of local and foreign vehicles by national authorities;
- vehicle manufacturing, in-life maintenance and end-of-life identification (vehicle life cycle management);
- adaptation of vehicle data (e.g. for international resales);
- safety-related purposes;
- crime reduction;
- commercial services.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN ISO 24534-4:2010
<https://standards.iteh.ai/catalog/standards/sist/c375ce03-e6ac-4289-8693-738a2136ab46/sist-en-iso-24534-4-2010>

It adheres to privacy and data protection regulations.

This part of ISO 24534 specifies the interfaces for a secure exchange of data between an ERT and an ERI reader or ERI writer in or outside the vehicle using asymmetric encryption techniques.

NOTE 1 The onboard device containing the ERI data is called the electronic registration tag (ERT).

This part of ISO 24534 includes:

- the application layer interface between an ERT and an onboard ERI reader or writer;
- the application layer interface between the onboard ERI equipment and external ERI readers and writers;
- security issues related to the communication with the ERT.

NOTE 2 The vehicle identifiers and possible additional vehicle data (as typically contained in vehicle registration certificates) are defined in ISO 24534-3.

NOTE 3 The secure application layer interfaces for the exchange of ERI data with an ERI reader or writer are specified in both this part of ISO 24534 and ISO 24534-5.

ISO 24534-4:2010(E)**2 Normative references**

The following referenced documents are indispensable for the application 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 8824 (all parts), *Information technology — Abstract Syntax Notation One (ASN.1)*

ISO/IEC 8825-2, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

ISO/IEC 14443 (all parts), *Identification cards — Contactless integrated circuit cards — Proximity cards*

ISO 15628:2007, *Road transport and traffic telematics — Dedicated short range communication (DSRC) — DSRC application layer*

3 Terms and definitions

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

3.1 access control
prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

[ISO 7498-2:1989, definition 3.3.1]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.2 access control list
list of entities, together with their access rights, which are authorized to have access to a resource

[ISO 7498-2:1989, definition 3.3.2]

SIST EN ISO 24534-4:2010
<https://standards.iteh.ai/catalog/standards/sist/c575cc05-60ac-4287-8093-738a2136ab46/sist-en-iso-24534-4-2010>

3.3 active threat
threat of a deliberate unauthorized change to the state of the system

[ISO 7498-2:1989, definition 3.3.4]

EXAMPLE Examples of security-relevant active threats may include modification of messages, replay of messages, and insertion of spurious messages, masquerading as an authorized entity and denial of service.

3.4 additional vehicle data
ERI data in addition to the vehicle identifier

[ISO 24534-3:2008, definition 3.1]

3.5 air interface
conductor-free medium between onboard equipment (OBE) and the reader/interrogator through which the linking of the OBE to the reader/interrogator is achieved by means of electromagnetic signals

[ISO 14814:2006, definition 3.2]

3.6 authority
organization that is allowed by public law to identify a vehicle using ERI

3.7**authorization**

granting of rights, which includes the granting of access based on access rights

[ISO 7498-2:1989, definition 3.3.10]

3.8**certification authority**

natural or legal person trusted to create public key certificates

NOTE See also top-level certification authority and intermediate certification authority.

3.9**challenge**

data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier

[ISO/IEC 9798-1:1997, definition 3.3.5]

NOTE In this part of ISO 24534 the term challenge is also used in case an ERT does not have enabled encryption capabilities and the challenge is merely copied without any secret information applied.

3.10**ciphertext**

data produced, through the use of encipherment; the semantic content of the resulting data is not available

[ISO 7498-2:1989, definition 3.3.14]

3.11**claimant**

entity which is or represents a principal for the purposes of authentication

NOTE A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

[ISO/IEC 10181-2:1996, definition 3.10]

3.12**cleartext**

intelligible data, the semantic content of which is available

[ISO 7498-2:1989, definition 3.3.15]

3.13**confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2:1989, definition 3.3.16]

3.14**credentials**

data that is transferred to establish the claimed identity of an entity

[ISO 7498-2:1989, definition 3.3.17]

3.15**cryptography**

discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2:1989, definition 3.3.20]