INTERNATIONAL STANDARD

ISO 24534-5

First edition
2011-12-15

Intelligent transport systems — Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles —

Part 5: Secure communications using symmetrical techniques

Systèmes de transport intelligents — Identification automatique des véhicules et des équipements — Identification d'enregistrement électronique (ERI) pour les véhicules —

Partie 5: Communications sécurisées utilisant des techniques symétriques

Reference number
ISO 24534-5:2011(E)

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

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 24534-5 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This first edition of ISO 24534-5 cancels and replaces the first edition of ISO/TS 24534-5:2008.

ISO 24534 consists of the following parts, under the general title *Intelligent transport systems — 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 within 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), such as legal proof of vehicle identity with potential mandatory usages. There is a commercial and economic justification both in respect of tags and infrastructure that a standard enable 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 an enabling technology for the future management and administration of traffic and transport, including applications in free flow, multi-lane, traffic conditions with the capability of supporting mobile transactions. ERI addresses the need of authorities and other users for a trusted electronic identification, including roaming vehicles.

This part of ISO 24534 specifies the interfaces for the exchange of data between an onboard component containing the ERI data and an ERI reader or writer inside or outside the vehicle using symmetric cryptographic techniques.

The exchanged identification data consists of a unique vehicle identifier and can also include data typically found in the vehicle's registration certificate (see ISO 24534-3 for details). The authenticity of the exchanged vehicle data can be further enhanced by using symmetric encryption techniques, i.e. techniques based on secret keys shared by a particular community of users.

The ERI interface defined in this part of ISO 24534 supports confidentiality measures to adhere to international and national privacy regulations and to prevent other misuse of electronic identification of vehicles.

Following the events of September 11th, 2001, and the subsequent reviews of anti-terrorism measures, the need for ERI has been identified as a possible anti-terrorism measure. The need for international 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. In addition, it includes provisions for security and the use of additional registration data of a vehicle.

Intelligent transport systems — Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles —

Part 5: Secure communications using symmetrical techniques

1 Scope

This International Standard provides the requirements for an electronic registration identification (ERI) using symmetric encryption techniques 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. in case of international re-sales,

— safety related purposes,

— crime reduction,

— commercial services, and

— adhering to privacy and data protection regulations.

This part of ISO 24534 specifies the interfaces for a secure exchange of data between the electronic registration tag (ERT), which is the onboard device containing the ERI data, and the ERI reader or ERI writer in or outside the vehicle using symmetric encryption techniques.

Symmetric encryption techniques are based on secret keys shared by a particular community of users, i.e. in closed user groups in which it is trusted that keys are not revealed to outsiders.

It includes

— the interface between an ERT and an onboard ERI reader or writer,

— the interface between the onboard ERI equipment and (roadside) reading and writing equipment, and

— security issues related to the communication with the ERT.

NOTE The vehicle identifiers and possible related vehicle information (as typically contained in a vehicle registration certificate) are defined in ISO 24534-3.

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

ISO 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

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

EN 12834, *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, definition 3.3.1]

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, definition 3.3.2]

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

[ISO 7498-2, definition 3.3.4]

EXAMPLE Modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity and denial of service.

3.4
additional vehicle data
electronic registration identification (ERI) data in addition to the vehicle identifier

[ISO 24534-3, definition 3.1]

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

[ISO 14814, definition 3.2]

3.6
authorization
granting of rights, which includes the granting of access based on access rights

[ISO 7498-2, definition 3.3.10]

3.7
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 9798-1, 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.

3.8
ciphertext
data produced, through the use of encipherment, the semantic content of which is not available

[ISO 7498-2, definition 3.3.14]

3.9
claimant
entity which is or represents a principal for the purposes of authentication, including the functions necessary for engaging in authentication exchanges on behalf of a principal

[ISO/IEC 10181-2, definition 3.10]

3.10
cleartext
intelligible data, the semantic content of which is available

[ISO 7498-2, definition 3.3.15]

3.11
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2, definition 3.3.16]

3.12
data integrity
integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2, definition 3.3.21]

3.13
decipherment
decryption
reversal of a corresponding reversible encipherment

[ISO 7498-2, definition 3.23]

3.14
distinguishing identifier
information which unambiguously distinguishes an entity

[ISO 9798-1, definition 3.3.9]

3.15
electronic registration identification
ERI
action or act of identifying a vehicle with electronic means for purposes as mentioned in the scope of this part of ISO 24534

3.16
electronic registration reader
ERR
device used to read or read/write data from or to an electronic registration tag (ERT)

NOTE 1 An ERR communicates directly, i.e. via an OSI data-link, with an ERT.

NOTE 2 An ERR can also be an ERI reader and/or an ERI writer or can act as a relay in the exchange of ERI data protocol units between an ERT and an ERI reader/writer.

3.17
electronic registration tag
ERT
onboard ERI device that contains the ERI data, including the relevant implemented security provisions and one or more interfaces to access that data

NOTE 1 In case of high security, the ERT is a type of secure application module (SAM).

NOTE 2 The ERT can be a separate device or can be integrated into an onboard device that also provides other capabilities (e.g. DSRC communications).

3.18
encipherment
encryption
cryptographic transformation of data to produce ciphertext

NOTE 1 Encipherment can be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

NOTE 2 Adapted from ISO 7498-2, definition 3.3.27.

3.19
end-to-end encipherment
encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system

[ISO 7498-2, definition 3.3.29]

3.20
entity authentication
corroboration that an entity is the one claimed

[ISO 9798-1, definition 3.3.11]

3.21
ERI data
vehicle identifying data which can be obtained from the ERT that consists of the vehicle identifier and possible additional vehicle data

NOTE Adapted from ISO 24534-3, definition 3.4.

3.22
ERI reader
device used to read ERI data directly or indirectly from an ERT by invoking ERI transactions

NOTE 1 In case an ERI reader exchanges the ERI protocol data units directly via a data link with an ERT, it is also called an ERR. In case it communicates via one or more nodes, only the last node in this sequence is called an ERR. As a consequence, an external ERI reader can, depending on the onboard configuration, act for some vehicles as an ERR and for others not.

NOTE 2 See also onboard ERI reader and external ERI reader.

3.23
ERI system operator
organization responsible for the operation of the ERI system and acting as the security authority for the ERI security domain

3.24
ERI writer
device used to write ERI data directly or indirectly into an ERT by invoking ERI transactions

NOTE 1 In case an ERI writer exchanges the ERI protocol data units directly via a data link with an ERT, it is also called an ERR. In case it communicates via one or more nodes, only the last node in this sequence is called an ERR. As a consequence, an external ERI writer can, depending on the onboard configuration, act for some vehicles as an ERR and for others not.

NOTE 2 See also onboard ERI writer and external ERI writer.

3.25
external ERI reader
ERI reader that is not part of the onboard ERI equipment

NOTE 1 An external ERI reader is not fitted within or on the outside of the vehicle.

NOTE 2 A distinction is made between proximity, short-range (DSRC), and remote external readers. A proximity reader can e.g. be a PCD (Proximity Coupling Device) as specified in ISO 14443. A short-range external ERI reader can be (a part of) roadside equipment, hand-held equipment, or mobile equipment. A remote external ERI reader can be part of the back-office equipment (BOE).

3.26
external ERI writer
ERI writer that is not part of the onboard ERI equipment

NOTE 1 An external ERI writer is not fitted within or on the outside of the vehicle.

NOTE 2 A distinction is made between proximity, short-range (DSRC), and remote external writers. A proximity reader can e.g. be a proximity coupling device (PCD) as specified in ISO 14443. A short-range external ERI writer can be (a part of) roadside equipment, hand-held equipment, or mobile equipment. A remote external ERI writer can be part of the back-office equipment (BOE).

3.27
identification
action or act of establishing identity

NOTE See also vehicle identification.

3.28
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification)

[ISO 9798-1, definition 3.3.13]

3.29
lifetime
period of time during which an item of equipment exists and functions

NOTE Adapted from ISO 14815, definition 4.8.

3.30
manipulation detection
mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally)

[ISO 7498-2, definition 3.3.35]

3.31
masquerade
pretence by an entity to be a different entity

[ISO 7498-2, definition 3.3.36]

3.32
mutual authentication
entity authentication which provides both entities with assurance of each other's identity

[ISO 9798-1, definition 3.3.14]

3.33
onboard ERI equipment
equipment fitted within or on the outside of the vehicle and used for ERI purposes

NOTE The onboard ERI equipment comprises an ERT and can also comprise any additional communication devices.

3.34
onboard ERI reader
ERI reader being part of the onboard ERI equipment

NOTE An onboard ERI reader can e.g. be a proximity coupling device (PCD) as specified in ISO 14443.

3.35
onboard ERI writer
ERI writer being part of the onboard ERI equipment

NOTE An onboard ERI writer can e.g. be a proximity coupling device (PCD) as specified in ISO 14443.

3.36
passive threat
threat of unauthorized disclosure of information without changing the state of the system

[ISO 7498-2, definition 3.3.38]

3.37
principal
entity whose identity can be authenticated

[ISO/IEC 10181-2, definition 3.15]

3.38
privacy
right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

NOTE Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

[ISO 7498-2, definition 3.3.43]

3.39
random number
time-variant parameter whose value is unpredictable

[ISO 9798-1, definition 3.3.24]

3.40
registration authority
organization responsible for writing the ERI data and security data into an ERT according to local legislation

NOTE It is expected that the registration authority with respect to the ERI data can be the same authority that keeps the official register in which the vehicle and its owner or lessee are listed. This is, however, not required by this part of ISO 24534.

3.41
secret key
key that is used with a symmetric cryptographic algorithm

NOTE 1 Possession of a secret key is restricted (usually to two entities).

NOTE 2 For ERI, there can be only one entity or several entities, depending on the key management policy.

NOTE 3 Adapted from ISO/IEC 10181-1, definition 3.3.15.

3.42
security

protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them

[ISO 12207, definition 4.39]

NOTE Security versus safety (informal):

Security: protection of a system against its environment; in this context the protection of the ERI system against attacks or accidents;

Safety: protection of the environment against a system; in this context the protection of the driver, passengers, vehicle, etc., against dangers of the ERI system.

3.43
security authority
entity that is responsible for the definition, implementation or enforcement of security policy

[ISO/IEC 10181-1, definition 3.3.17]

3.44
security domain
set of elements, security policy, security authority and set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

[ISO/IEC 10181-1, definition 3.3.20]

3.45
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO 7498-2, definition 3.3.51]