TECHNICAL SPECIFICATION

ISO/TS 24534-4

First edition
2008-02-15

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

Part 4: Secure communications using asymmetrical techniques

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

Partie 4: Communications sûres utilisant des techniques asymétriques

Reference number
ISO/TS 24534-4:2008(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.

COPYRIGHT PROTECTED DOCUMENT

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.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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/TS 24534-4 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, and by Technical Committee CEN/TC 278, *Road transport and traffic telematics* in collaboration.

ISO/TS 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 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/benefits of 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 enables an interoperable solution.

Electronic Registration Identification (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 to support mobile transactions. ERI addresses the need of authorities and other users for a trusted electronic identification, including roaming vehicles.

This part of ISO/TS 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) re-sales 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 Technical Specification 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/TS 24534 makes use of the basic automatic vehicle identification (AVI) provisions already defined in ISO 14814 and 14816.

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

Part 4:
Secure communications using asymmetrical techniques

1 Scope

This part of ISO/TS 24534 provides the requirements for an Electronic Registration Identification (ERI) that is 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, and
- commercial services.

It adheres to privacy and data protection regulations.

This part of ISO/TS 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 Technical Specification 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, and
- 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/TS 24534-3.

NOTE 3 The secure application layer interfaces for the exchange of ERI data with an ERI reader or writer are specified in ISO/TS 24534-4 and a future ISO/TS 24534-5.

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 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

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 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General*

ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security framework for open systems: Authentication framework*

ISO/IEC 10646:2003, *Information technology — Universal Multiple-Octet Coded Character Set (UCS)*

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

ISO/CD 14814, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology*

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

ISO 15628, *Transport Information and Control Systems (TICS) — 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 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, 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 electro-magnetic signals

[ISO 14814, definition 3.2]

3.6
authority
organisation 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, 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 9798-1, definition 3.3.5]

NOTE In this Technical specification 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, 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 10181-2, definition 3.10]

3.12
cleartext
intelligible data, the semantic content of which is available

[ISO 7498-2, 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, definition 3.3.16]

3.14
credentials
data that is transferred to establish the claimed identity of an entity

[ISO 7498-2, 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, definition 3.3.20]

3.16
data integrity
integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2, definition 3.3.21]

3.17
decipherment
decryption
reversal of a corresponding reversible **encipherment**

[ISO 7498-2, definition 3.3.23]

3.18
digital signature
signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

NOTE See also **cryptography**.

[ISO 7498-2, definition 3.3.26]

3.19
distinguishing identifier
information which unambiguously distinguishes an entity

[ISO/IEC 9798-1, definition 3.3.9]

3.20
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/TS 24534

3.21
electronic registration reader
ERR
device used to read or read/write data from or to an **ERT**

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

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

3.22
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 An implementer may choose also to integrate other provisions (e.g. for DSRC communications) into an ERT as long as this does not compromise the security of the ERT.

3.23
encipherment
encryption
cryptographic transformation of data to produce **ciphertext**

[ISO 7498-2, definition 3.3.27]

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

NOTE 2 See also **cryptography**.

[ISO 7498-2]

3.24
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]

3.25
entity authentication
corroboration that an entity is the one claimed

[ISO/IEC 9798-1, definition 3.3.11]

3.26
ERI data
vehicle identifying data which can be obtained from an **ERT**

NOTE ERI data consist of the vehicle identifier and possible additional vehicle data.

3.27
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 may e.g. 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.

3.28
ERI transaction
transaction as defined in Clause 6 of this part of ISO/TS 24534

3.29
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 may, e.g. 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**.

3.30
ERT holder
legal or natural person holding an ERT

NOTE The ERT holder could be, for example, the holder of the registration number or the owner, operator or keeper of the vehicle.

3.31
ERT number
number assigned to and written into an ERT that acts as an ERT unique identifier

NOTE The ERT number is assumed to be written into the ERT during its manufacture and once written cannot be changed.

3.32
external ERI reader
an **ERI reader** not being 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 may e.g. be a PCD (Proximity Coupling Device) as specified in ISO 14443. A short-range external ERI reader may be a part of roadside equipment, hand-held equipment, or mobile equipment. A remote external ERI reader may be part of the back-office equipment (BOE).

3.33
external ERI writer
ERI writer not being 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 may e.g. be a PCD (Proximity Coupling Device) as specified in ISO 14443. A short-range external ERI writer may be (a part of) roadside equipment, hand-held equipment, or mobile equipment. A remote external ERI writer may be part of the back-office equipment (BOE).

3.34
hash-code
string of bits which is the output of a **hash-function**

3.35
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

a) for a given output, it is computationally infeasible to find an input which maps to this output; and

b) for a given output, it is computationally infeasible to find a second input which maps to the same output

[ISO/IEC 10118-1, definition 3.5]

NOTE Computational feasibility depends on the specific security requirements and environment.

3.36
identification
action or act of establishing the identity

NOTE See also **vehicle identification**.

3.37
intermediate certification authority
certification authority for which **public key certificates** are issued by the **top-level certification authority**

NOTE This definition implies that there can be only one "level" of intermediate certification authorities.

3.38
key
sequence of symbols that controls the operations of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function, signature generation, or signature verification)

[ISO 9798-1, definition 3.3.13]

NOTE See ISO 9798-1 for the meaning of the terms used for the examples of cryptographic transformations.

3.39
lifetime
period of time during which an item of equipment exists and functions

NOTE Adapted from ISO 14815.

3.40
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]

3.41
masquerade
pretence by an entity to be a different entity

[ISO 7498-2, definition 3.3.36]

3.42
non-repudiation
property that none of the entities involved in a communication can deny in all or in part its participation in the communication

NOTE Adapted from ISO 7498-2.

3.43
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 may also comprise any additional communication devices.

3.44
onboard ERI reader
ERI reader which is part of the **onboard ERI equipment**

NOTE An onboard ERI reader could be, for example, a proximity coupling device (PCD) as specified in ISO 14443.

3.45
onboard ERI writer
ERI writer which is part of the **onboard ERI equipment**

NOTE An onboard ERI writer could be, for example, a proximity coupling device (PCD) as specified in ISO 14443.

3.46
passive threat
threat of unauthorized disclosure of information without changing the state of the system

[ISO 7498-2, definition 3.3.38]

3.47
password
confidential authentication information, usually composed of a string of characters

[ISO 7498-2, definition 3.3.39]

3.48
periodic motor vehicle test
compulsory periodic (e.g. annual) test of the roadworthiness of a motor vehicle of above a specified age, or a certificate of passing such a test

EXAMPLE The MOT test in the United Kingdom is an example.

3.49
principal
entity whose identity can be authenticated

[ISO/IEC 10181-2, definition 3.15]

3.50
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

[ISO 7498-2, definition 3.3.43]

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.

3.51
private decipherment key
private key which defines the private decipherment transformation

[ISO/IEC 9798-1, definition 3.3.16]

3.52
private key
key of an entity's asymmetric key pair which should only be used by that entity

[ISO/IEC 9798-1, definition 3.3.17]

NOTE In the case of an asymmetric signature system the private key defines the signature transformation. In case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.53
private signature key
private key which defines the private signature transformation

[ISO/IEC 9798-1, definition 3.3.18]

3.54
public encipherment key
public key which defines the public encipherment transformation

[ISO/IEC 9798-1, definition 3.3.19]

3.55
public key
key of an entity's asymmetric key pair which can be made public

NOTE In the case of an asymmetric signature system the public key defines the verification transformation. In case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is "publicly" known is not necessarily globally available. The key may only be available to all members of a pre-specified group.

[ISO/IEC 9798-1, definition 3.3.20]

3.56
public key certificate
certificate
public key information of an entity signed by the certification authority and therefore rendered unforgeable

[ISO/IEC 9798-1, definition 3.3.21]

NOTE In this Technical Specification, a public key certificate also specifies the role of the entity for which the public key information is provided, e.g. manufacturer or registration authority.

3.57
public verification key
public key which defines the public verification transformation

[ISO/IEC 9798-1, definition 3.3.23]

3.58
random number
time variant parameter whose value is unpredictable

[ISO/IEC 9798-1, definition 3.3.24]

3.59
registration authority (with respect to the ERI data)
organization responsible for writing **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 may be the same authority that keeps the official register in which the vehicle and its owner or lessee are listed. This part of ISO/TS 24534 does not require this, however.

3.60
registration certificate
document (paper or smart card) which certifies that the vehicle is registered in a state or country