

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

## Part 4: Secure communications using asymmetrical techniques

ICS 03.220.20; 35.240.60

National foreword

This Draft for Development is the UK implementation of CEN ISO/TS 24534-4:2008.

**This publication is not to be regarded as a British Standard.**

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the European organization responsible for its conversion to a European standard. A review of this publication will be initiated not later than three years after its publication by the European organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into a European Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Road transport informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 March 2008

© BSI 2008

ISBN 978 0 580 54816 1

Amendments/corrigenda issued since publication

| Date | Comments |
|------|----------|
|      |          |
|      |          |
|      |          |
|      |          |

English Version

**Automatic vehicle and equipment identification - Electronic  
Registration Identification (ERI) for vehicles - Part 4: Secure  
communications using asymmetrical techniques (ISO/TS 24534-  
4:2008)**

Identification automatique des véhicules et des  
équipements - Identification d'enregistrement électronique  
(ERI) pour les véhicules - Partie 4: Communications sûres  
utilisant des techniques asymétriques (ISO/TS 24534-  
4:2008)

Straßenverkehrstelematik (RTTT) - Automatische  
Identifizierung von Fahrzeugen und Ausrüstungen -  
Elektronische Identifizierung für die Registrierung (ERI) -  
Teil 4: Sichere Anwendungsebene mittels asymmetrischer  
Techniken (ISO/TS 24534-4:2008)

This Technical Specification (CEN/TS) was approved by CEN on 17 July 2006 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, 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: rue de Stassart, 36 B-1050 Brussels**

## **Foreword**

This document (CEN ISO/TS 24534-4:2008) 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 "Transport information and control systems".

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.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Bulgaria, 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.

## Contents

Page

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>Foreword</b> .....                                    | <b>iv</b> |
| <b>Introduction</b> .....                                | <b>v</b>  |
| <b>1 Scope</b> .....                                     | <b>1</b>  |
| <b>2 Normative references</b> .....                      | <b>2</b>  |
| <b>3 Terms and definitions</b> .....                     | <b>2</b>  |
| <b>4 Abbreviations</b> .....                             | <b>11</b> |
| <b>5 System communications concept</b> .....             | <b>12</b> |
| 5.1 Introduction .....                                   | 12        |
| 5.2 Overview .....                                       | 12        |
| 5.3 Security services .....                              | 19        |
| 5.4 Communication architecture description.....          | 24        |
| 5.5 Interfaces .....                                     | 26        |
| <b>6 Interface requirements</b> .....                    | <b>27</b> |
| 6.1 Overview .....                                       | 27        |
| 6.2 Abstract transaction definitions.....                | 28        |
| 6.3 The ERT interfaces .....                             | 65        |
| <b>Annex A (normative) ASN.1 Modules</b> .....           | <b>69</b> |
| <b>Annex B (informative) Operational scenarios</b> ..... | <b>80</b> |
| <b>Annex C (normative) PICS pro forma</b> .....          | <b>91</b> |
| <b>Bibliography</b> .....                                | <b>95</b> |

## 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

**3.61**

**replay attack**

**masquerade** which involves use of previous transmitted messages

[ISO/IEC 9798-1, definition 3.3.26]

**3.62**

**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/IEC 12207, definition 3.25]

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.

**3.63**

**sequence number**

time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

[ISO/IEC 9798-1, definition 3.3.27]

**3.64**

**threat**

potential violation of security

[ISO 7498-2, definition 3.3.55]

**3.65**

**top-level certification authority**

certification authority whose certificates can be verified because its public verification key(s) are written as read-only data into the **ERT** before the ERT is customised or commissioned

**3.66**

**unilateral authentication**

entity authentication which provides one entity with the assurance of the other's identity but not vice versa

[ISO/IEC 9798-1, definition 3.3.33]

**3.67**

**vehicle identification**

action or act of establishing the identity of a vehicle

**3.68**

**verifier**

entity which is or represents the entity requiring an authenticated identity

NOTE A verifier includes the functions necessary for engaging in authentication exchanges.

[ISO/IEC 10181-2, definition 3.20]

## 4 Abbreviations

### 4.1

#### **AEI**

Automatic Equipment Identification

### 4.2

#### **AES**

Advanced Encryption Standard

### 4.3

#### **ASN.1**

Abstract Syntax Notation One

NOTE Defined in ISO/IEC 8824.

### 4.4

#### **AVI**

Automatic Vehicle Identification

### 4.5

#### **BOE**

Back Office Equipment

### 4.6

#### **EN**

Europäische Norm (German), English: European Standard

### 4.7

#### **ENV**

Europäische Norm Vorausgabe (German), English: European Pre-Standard

### 4.8

#### **ERI**

Electronic Registration Identification

### 4.9

#### **ERR**

Electronic Registration Reader: a device used to read or read/write data from or to an ERT

### 4.10

#### **ERT**

Electronic Registration Tag

### 4.11

#### **EU**

European Union

### 4.12

#### **IEC**

International Electrotechnical Commission

### 4.13

#### **ISO**

International Organization for Standardization

### 4.14

#### **OBE**

On Board Equipment (including non-ERI equipment)

**4.15**

**OSI**

Open Systems Interconnection (see ISO/IEC 7498-1)

**4.16**

**PICS**

Protocol Implementation Conformance Statement(s)

**4.17**

**PIN**

Personal Identification Number

**4.18**

**SAM**

Secure Application Module

**4.19**

**VIN**

Vehicle Identification Number

## **5 System communications concept**

### **5.1 Introduction**

Clause 5 is informative only.

This Clause provides an introduction to the context in which ERI data and security data may be read from, or written into, the ERT and in which vehicles can be identified. It also outlines options that may or may not be used in an actual implementation. The normative requirements for the application layer interfaces are provided in Clause 6 and Annex A. Annex C (normative) contains a form to specify the limitations of an actual communication protocol implementation.

### **5.2 Overview**

#### **5.2.1 Vehicle registration identification**

ERI, Electronic Registration Identification, is the action or act of identifying a vehicle by electronic means for the purposes mentioned in the scope of this part of ISO/TS 24534.

The identifier used to identify a vehicle is called the vehicle identifier or vehicleId.

NOTE 1 The preferred vehicle identifier is the VIN that is assigned to the vehicle by its manufacturer in accordance with ISO 3779, but alternatives are supported as well (see ISO/TS 24534-3 for details).

NOTE 2 See ISO/TS 24534-3 for details about the vehicle identifier and ERI data.

In this part of ISO/TS 24534, the combination of the almost unique vehicleId and a unique ERT number is used as the unambiguous distinguishing identifier.

#### **5.2.2 System concept and supported interfaces**

Figure 1 presents the interfaces for which the application layer is specified in this part of ISO/TS 24534.

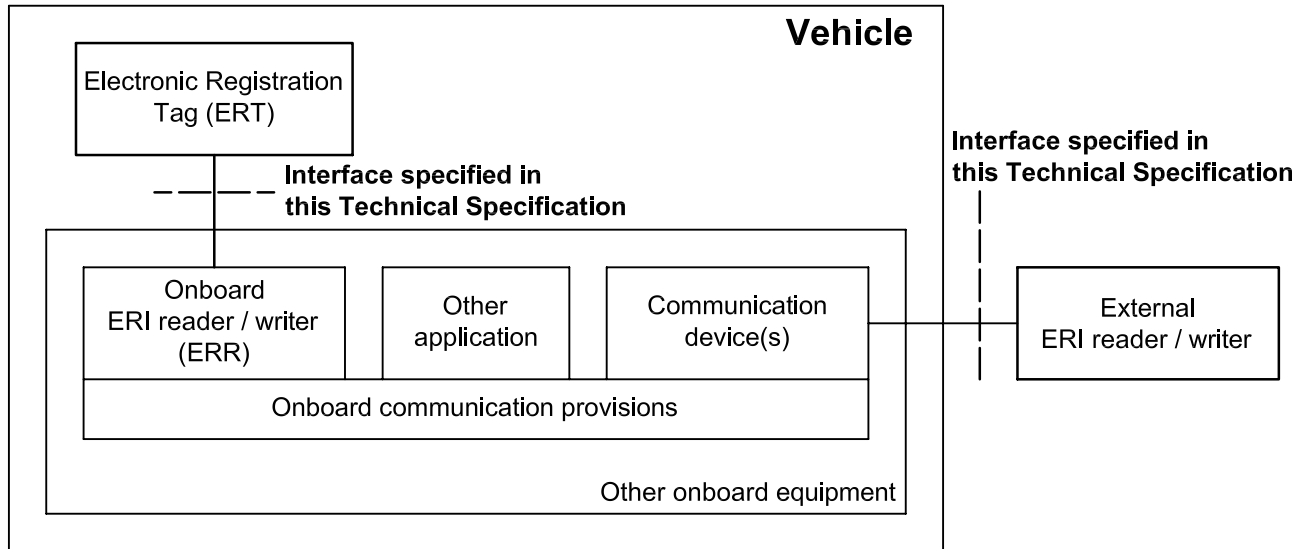


**Figure 1 — System concept and supported interfaces**

The onboard component that provides a secure environment for the ERI data and security data is called the Electronic Registration Tag (ERT).

NOTE 1 An implementer may integrate other provisions (e.g. additional communication provisions) into an ERT as long as this does not compromise the security of the ERT.

Depending on its capabilities, an ERT is tailored to a specific vehicle in three consecutive steps (see also Figure B.2 — ERT state diagram):

- a) First, it is customized with the vehicle identifier and, optionally, additional vehicle data. This step can only be performed once in the lifetime of an ERT. Customizing does not yet enable any ERT encipherment or signing services.
- b) Second, a registration authority may commission itself as the registration authority for the vehicle by adding its security data. This step may be performed at any time by a registration authority when it wants to commission itself as the current registration authority. A registration authority may change its security data by re-commissioning itself. If supported by the ERT, commissioning enables ERT confidentiality and authentication services by providing the required security keys. If a key is not provided, the corresponding services will not be enabled.

NOTE 2 Most smart cards are “owned” and “controlled” by one issuer during their whole life time. For an ERT this is more complicated. When an vehicle is sold to another country a new registration authority will just take over the “control” or “ownership” of the ERT when it issues a new number plate and a new registration certificate for the vehicle. The ERT is then re-commissioned.

- c) Third, a registration authority that has commissioned itself may change the additional vehicle data to register a change of the vehicle data (with the exception of the vehicleId).

NOTE 3 In order to accommodate the needs of different countries, different selections of additional vehicle data can be included. (See ISO/TS 24534-3 for details.)

The onboard communication provisions shall be able of transferring data from or to the ERT without modifying that data.

NOTE 4 The onboard communication provisions may e.g. be part of an onboard platform for transport applications.

A communication device may communicate with an external proximity reader or writer, with a short range ERI reader and/or writer, or with remote back office equipment (BOE).

A communication device that communicates with an external ERI reader/writer acts as a relay between this external ERI reader/writer and the onboard ERI reader/writer. A communication device may also be used for other applications.

### 5.2.3 Roles involved

Within the context of this part of ISO/TS 24534 the following “roles” for natural or legal persons are distinguished:

- Manufacturers, who assign a VIN or chassis number to each vehicle they build. A manufacturer may also once customize an ERT for a particular vehicle.
- Registration authorities (with respect to the ERI data), who may:
  - assign a new vehicleId to the vehicle (in case of defects) and may customize an ERT (e.g. in the case of defects or retrofitting),

NOTE A registration authority may assign a new vehicle id to the vehicle (e.g. when the number on the chassis has become corrupted). Then he will put that new id on the chassis and write it in a new ERT (a vehicle id can never be overwritten)

- commission itself as the registration authority for a vehicle,
- authorize other authorities to read the ERI data,
- authorize an ERT holder to grant additional service providers access to ERI data, and

who are responsible for the registration of additional vehicle data into an ERT according to local legislation (see below for details).

NOTE 1 It is expected that the registration authority with respect to the ERI data is the same authority that keeps the official register in which the vehicle is listed. This is however not required by this part of ISO/TS 24534.

NOTE 2 It is assumed that each vehicle is listed in a register that contains the vehicle identifier and additional data related to the vehicle. It is implicitly assumed that this register also identifies the one(s) responsible for the vehicle (e.g. its owner, operator, keeper, lessee, and/or regular driver).

- Certification authorities, who are trusted to create public key certificates (referred to as “certificates” in this part of ISO/TS 24534). Public key certificates are used to prevent a fraudulent organization from disguising itself as a manufacturer or registration authority. There are two types of certification authorities:
  - one top-level certification authority, and
  - zero or more intermediate certification authorities.

NOTE 3 A certification authority will not directly communicate with the ERT. Their certificates are used by manufacturers and registration authorities.

NOTE 4 With two levels of certification authority, the top-level authority can delegate the distribution of certificates to an intermediate authority, which is then responsible for creating the certificates for registration authorities and manufacturers within some region (e.g. the states of the United States or the member states of the EU).

- Authorities, who are authorized by the registration authority to read the ERI data from a vehicle (e.g. because they are entitled to do so by virtue of public legislation).
- Additional service providers (public or private), who provide a service which requires an electronic identification of a vehicle and/or certificated vehicle data. The ERT holder may or may not authorize an additional service provider to read the vehicle's identifier and the additional vehicle data.

- ERT holders, who are holding the ERT. An ERT holder may e.g. be the holder of the vehicle's registration number or the owner, operator, or keeper of the vehicle.

Even in cases where confidentiality of the ERI data is supported, the ERT holder is entitled both to read the ERI in its vehicle and to allow other service providers to read the vehicle identifier. A PIN issued by the registration authority to the ERT holder provides the required access control for the ERT holder.

NOTE 5 Roles and requirements related to the specification, design and manufacturing (including testing) of an ERT are outside the scope of this part of ISO/TS 24534.

#### 5.2.4 The communications context for reading

Figure 2 shows the communications context for reading data from an ERT.

An onboard or an external ERI reader is used to read data from the ERT. An onboard ERI reader communicates directly with the ERT. An external ERI reader may communicate either directly or indirectly with the ERT, e.g. directly in the case of a hand-held reader or an integrated ERI device, or indirectly via an onboard communication module and the onboard ERI reader. The onboard communication module may also be used for other applications.

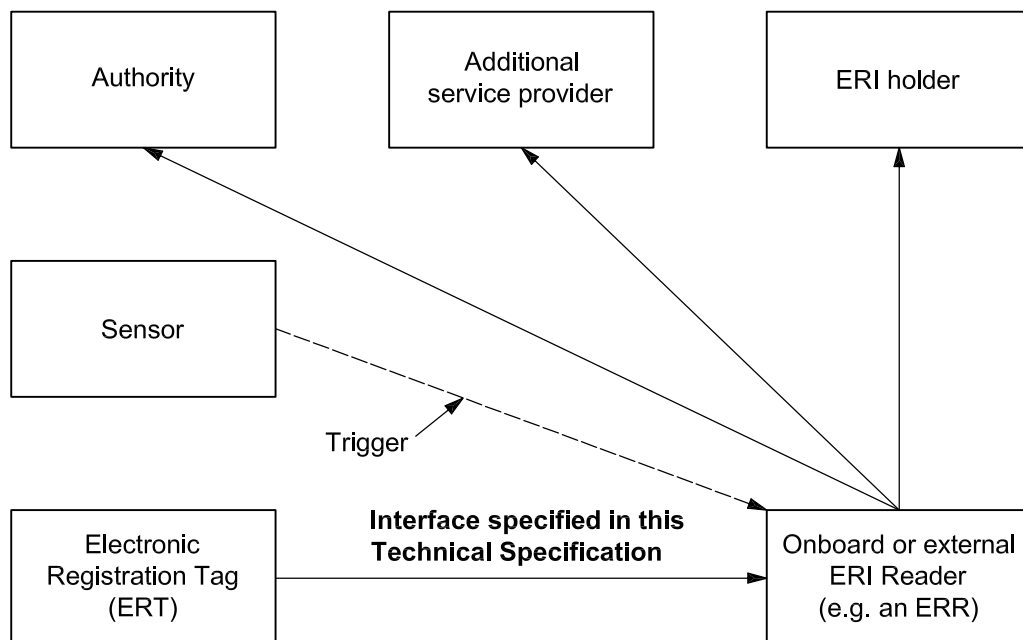


**Figure 2 — Communication context for reading from an ERT**

A sensor system (outside the scope of this Technical Specification) may be used to trigger an external ERI reader when it senses the presence of a vehicle that needs to be identified.

The various parties that can read ERI data from an ERT are described in 5.2.3. The access rights of the various entities are described in 5.3.5.1.

An ERT holder may wish to have access to the ERI data for various reasons:

- to verify the correctness of the ERI data;
- to obtain an authenticated (i.e. signed) vehicle identifier or ERI data to be used for another application;
- to verify the access control list (see 5.3.5), if present in the ERT;
- to verify the historic ERI data and/or historic commissioning data, if present in the ERT.

The equipment used by an authority, additional service provider or ERT holder in his office (i.e. not at the roadside) is called Back Office Equipment (BOE).

The distribution of functions between BOE and an external ERI reader is outside the scope of this Technical Specification.

### 5.2.5 The communications context for writing

Figure 3 presents the communications context for writing data into an ERT.

The onboard or external ERI writer is used to write data into the ERT. An onboard ERI writer communicates directly with the ERT. An external ERI writer may communicate either directly or indirectly with the ERT, e.g. directly in the case of a hand-held writer or an integrated ERI device, or indirectly via an onboard communication module and the onboard ERI writer. The onboard communication module may also be used for other applications.

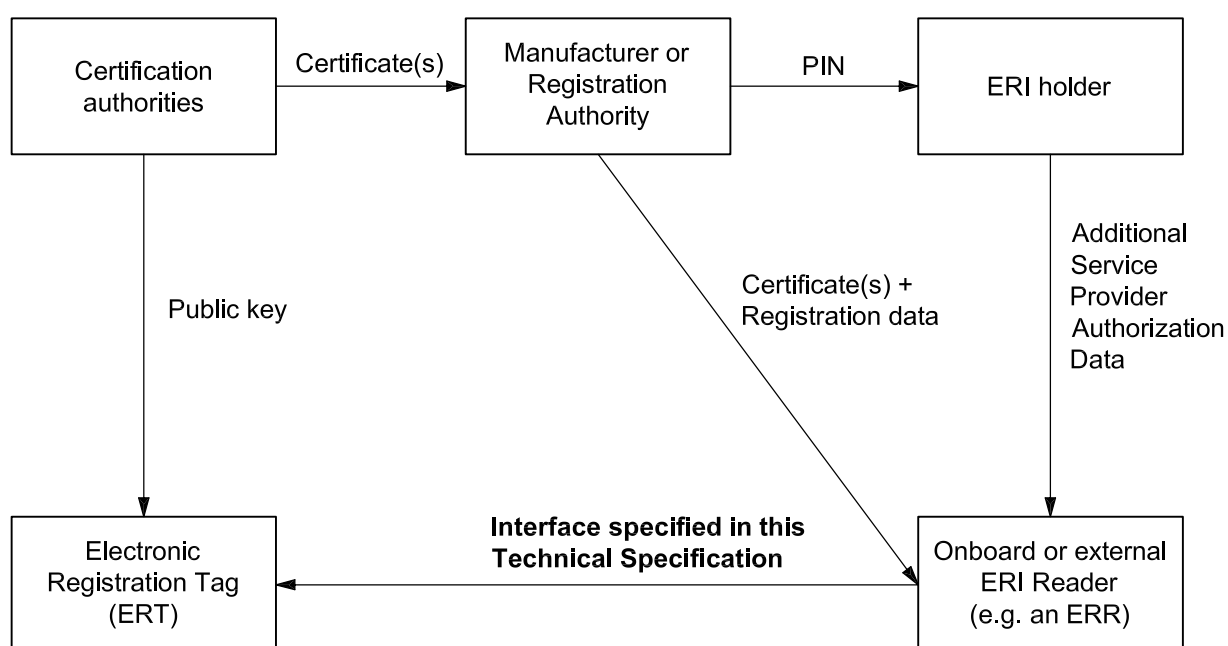


**Figure 3 — Communication context for writing into an ERT**

The various parties that can write ERI (security) data into an ERT are described in 5.2.3. The access rights of the various entities are described in 5.3.5.2.

The certification authorities provide public key certificates for genuine manufacturers and genuine registration authorities. The certificates are used while writing data into the ERT in order to prove that (signed) data originates from a genuine manufacturer or genuine registration authority. The certificates are also used while the ERI data is read in order to check that the data received stems from a genuine ERT, manufacturer or registration authority.

The Registration Authority authorizes the ERT holder by providing a password (PIN). The ERT holder may then authorize an additional service provider to read ERI data.

The distribution of functions between BOE and an external ERI writer is outside the scope of this Technical Specification. A registration authority may e.g. commission a writer to operate on its behalf or it may use e.g. the writer only as a relay device for remote writing from its back office.

### 5.2.6 ERT capability levels supported

It is envisioned that different users may have different requirements for ERI. Therefore, this part of ISO/TS 24534 supports different service levels of ERT capabilities.

Figure 4 presents an overview of the various capability levels supported by this part of ISO/TS 24534. See also Annex C with the Protocol Implementation Conformance Statements (PICS) proforma.

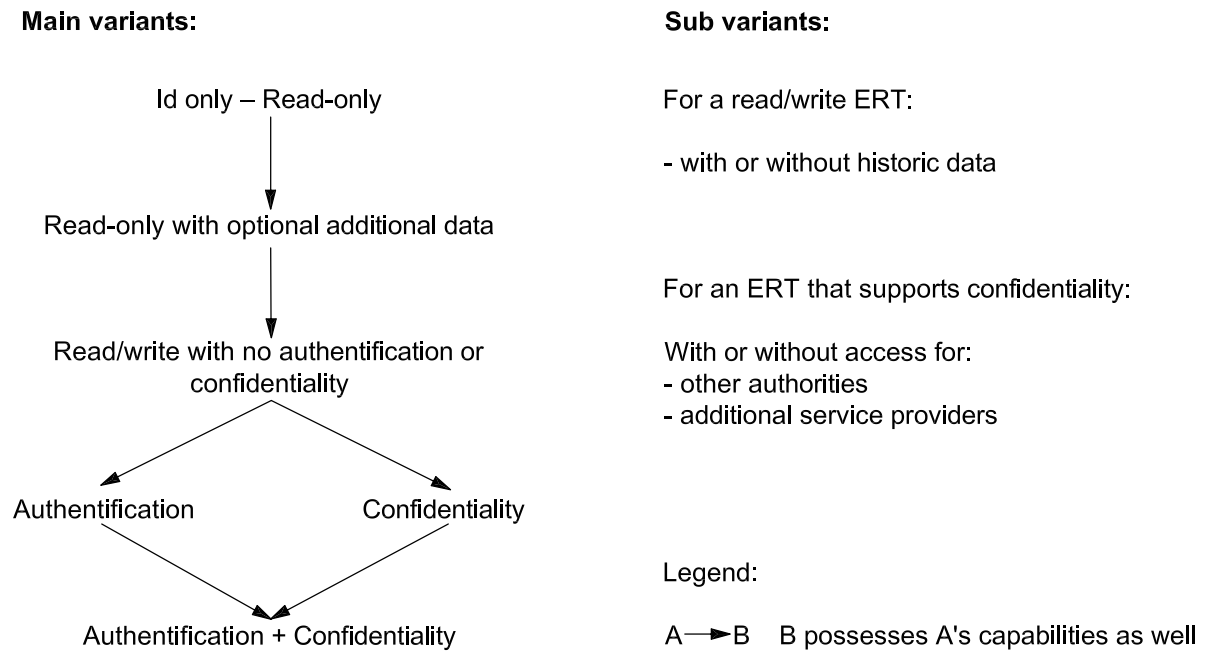


**Figure 4 — ERT capability levels supported**

The following main variants are distinguished (a variant at the arrowhead also includes the capabilities of the one at the arrow tail):

- **Id only – Read only:** This is the simplest ERT. The vehicle identifier is written only once and no other information can be added. In this case an ERI reader can only read the vehicle identifier from the vehicle (ERT).
- **Read only with optional additional vehicle data:** in this case the ERT may also contain additional vehicle data as specified in ISO/TS 24534-3. However, all data can only be written once in the lifetime of an ERT. For security reasons the data may also contain a signature from the origination entity.
- **Read/write with no authentication or confidentiality:** in this case the ERT contains the vehicle identifier plus optional additional vehicle data. This additional vehicle data can be updated if required.
- **Read/write with authentication:** in this case the ERT also provides authentication services. The ERT can check a signature attached to data written into it. If enabled, the ERT can also attach as signature to data it sends to an ERI reader. An ERI reader can then check that the data it receives stems from a genuine ERT and not from a fake one.

NOTE 1    A registration authority can disable the ERT signing capabilities but not the signature verification capabilities.

- **Read/write with confidentiality:** in this case the ERT is capable of providing confidentiality services. The ERT can decrypt security data encrypted by an ERD writer. If enabled, the ERT can also encrypt the data it sends to an ERI reader. This data can only be interpreted by those parties which possess the corresponding private decipherment key.

NOTE 2 A registration authority can disable the ERT encipherment capabilities but not the decipherment capabilities.

- Read/write with both authentication and confidentiality: in this case the ERT provides both authentication and confidentiality services.

In addition to these main variants, various sub variants may be distinguished, e.g.:

- A read/write ERT which also maintains a log of historic data, i.e. of previous write operations;
- An ERT with confidentiality services for which the registration authority can also authorize other authorities to read the ERI data;
- An ERT with confidentiality services for which the registration authority may also grant the ERT holder permission to read the (historic) ERI data in his ERT;
- An ERT with confidentiality services for which the registration authority may also grant the ERT holder permission to authorize additional service providers to read the ERI data in his ERT.

### 5.2.7 Security service levels and interoperability

This part of ISO/TS 24534 supports authorities in identifying vehicles roaming from the jurisdiction of other registration authorities. Therefore, much attention is given to the interoperability of ERTs and readers of various capability levels, i.e. the identification of a vehicle with a simple ERT by a sophisticated reader and vice versa.

The basic principle for the interoperability of ERTs and ERI readers is that the reader will function with the full range of capabilities of the ERT. If the reader does not provide full functionality, e.g. the required decipherment capabilities, then the authority using the reader may ask for (decipherment) assistance from the registration authority. A similar situation applies when the ERT signs data.

Table 1 presents the various combinations when an ERT and an ERI reader have different cryptographic capabilities.

**Table 1 — Interoperability between ERTs and ERI readers**

| ERT                 | ERI reader                    | Interoperability                                                                                                                              |
|---------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <u>Encipherment</u> | <u>Decipherment</u>           |                                                                                                                                               |
| Yes                 | No                            | The reader will not understand the ERI data, which needs the assistance of the vehicle's registration authority for decrypting the data read. |
| No                  | Yes                           | The reader does not need to use its decryption capabilities.                                                                                  |
| <u>Signing</u>      | <u>Signature verification</u> |                                                                                                                                               |
| Yes                 | No                            | The reader will not be able to check any signature provided for the ERI data.                                                                 |
| No                  | Yes                           | The reader does not need to use its signature verification capabilities.                                                                      |

In order to support readers with no decipherment capabilities, a registration authority may, if required, disable the encipherment capabilities of ERT for vehicles in his jurisdiction.

EXAMPLE When a vehicle is imported from a country with strict privacy protection into a country with less-strict privacy protection and which consequently employs readers with no decipherment capabilities, then the registration authorities may disable the decipherment capabilities of the ERT when it is commissioned.

NOTE 1 Harmonisation of the security requirements of the registration authority is outside the scope of this Technical Specification.

With respect to the interoperability between ERTs and ERI writers, precedence has been given to security above the support of international (re)sales. As a registration authority may replace an ERT, this is not considered to be a severe restriction. The basic principle for writing is that a writer and, hence, a registration authority can determine the capabilities of an ERT and based upon this, the registration authority can decide to accept that ERT or replace it with one that matches their requirements.

NOTE 2 If a registration authority does not accept a particular ERT, then that authority should replace it with one that is acceptable and customise it as necessary.

The interoperability of ERTs and ERI writers of various capability levels is depicted in Table 2.

**Table 2 — Interoperability between ERTs and ERI writers**

| ERI writer          | ERT                           | Interoperability                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>Encipherment</u> | <u>Decipherment</u>           |                                                                                                                                                                                                                                                                                                                                                                                   |
| Yes                 | No                            | The ERI writer can only write data into such an ERT if it disables its encipherment capabilities.                                                                                                                                                                                                                                                                                 |
| No                  | Yes                           | The ERT will not accept any data that has to be encrypted from such a writer.<br>More precise, the ERT will then not accept any private signature key or PIN in a commissioning transaction. As a consequence the invocation of a commissioning transaction will disable the ERT signing capabilities and will prevent the use of a PIN by an ERT holder.                         |
| <u>Signing</u>      | <u>Signature verification</u> |                                                                                                                                                                                                                                                                                                                                                                                   |
| Yes                 | No                            | The ERT will not verify any signature provided by the writer. As a consequence every writer can be used to change the ERI data and its security data.<br><br>NOTE This is not advisable, but allowed in this Technical Specification. It is the responsibility of the registration authority to allow or not to allow (i.e. to commission or not to commission) this kind of ERT. |
| No                  | Yes                           | The ERT will not accept any data from this writer.                                                                                                                                                                                                                                                                                                                                |

It is the responsibility of a registration authority to accept or not accept a particular ERT within his jurisdiction, i.e. a registration authority may or may not want to commission itself on a particular ERT.

### 5.3 Security services

#### 5.3.1 Assumptions

The security concept for the exchange of data between an ERT and an ERI reader or writer is based on the following assumptions:

- The use of an ERT may be mandatory and, therefore, should be fraud resistant. Using ISO/IEC 7498-2 terminology, the ERT should be resistant against active threats (e.g. modification of messages, replay of messages, insertion of spurious messages, and masquerading).
- A reading of an ERT should be suitable as legal evidence (non-repudiation).

NOTE This may require the specification of an Protection Profile (including an adequate Evaluation Assurance Level EAL) for the ERT according to ISO 15408. However, such a specification is outside the scope of this Technical Specification.

- ERI shall have the capability to provide a high level of privacy protection (i.e. it should not be easily possible to monitor mobility patterns of a vehicle and, hence, of its regular driver). As a consequence, an ERT should also be resistant against passive threats.

- ERI shall have the capability to provide protection measures to prevent ERI from being used to trigger an attack on a vehicle.
- The performance of security mechanisms must be achievable within the time available for communications whilst the vehicle is moving (a calculation example: reading a vehicle at 180 km/h within a 10 metres read range should be achieved within 200 ms).

### **5.3.2 Entity authentication while reading ERI data**

Trust in the authenticity of an ERI reading depends on the following authentication aspects, which must all be fulfilled to fully trust a reading:

- a) The ERT is customized with the correct vehicle identifier and is attached to the correct vehicle.
- b) The ERT cannot be removed from the vehicle without rendering it inoperable.
- c) The ERI data is read from a genuine ERT, i.e. from a legitimate device (it is not a replicated message from a fake one). This is achieved by signing the ERI data together with a challenge code provided by the ERI reader.
- d) The ERI data is correctly read from the ERT (data integrity, manipulation detection). This is achieved by standard mechanisms used in data communications, by signing data, and, as a side effect, by encrypting the ERI data (Decipherment of corrupted ciphertext will not produce anything useful).
- e) When ERI data has been correctly read from a genuine ERT upon a particular request it shall be difficult to be disputed later on that this data was not read from this component upon that request (non-repudiation). This is achieved by signing the ERI data together with a challenge code provided by the ERI reader.

NOTE 1 This Technical Specification only deals with c), d), and e). The item b) is specified in ISO/TS 23524-2. Item a) is not dealt with in this Technical Specification.

NOTE 2 Using ISO/IEC 9798-3 terminology, c) and e) are supported using a two-pass unilateral authentication mechanism. Uniqueness/timeliness is then controlled by generating and checking a random number sent by the ERI-reader (the verifier) to the ERT (the claimant).

### **5.3.3 Confidentiality while reading ERI data**

This Technical Specification supports confidentiality by delivering ERI data in an encrypted format. The encrypted ERI data can then be made freely available but can only be decrypted and interpreted by authorized persons/equipment (end-to-end encipherment).

To prevent that encrypted ERI data can be used as a pseudonym, a sequence number is added to the ERI data before encryption.

NOTE Confidentiality is, in more technical terms, provided by means of asymmetric keys. In the case of read operations the ERT uses a public encipherment key of an authority written into the ERT by the registration authority or by the ERT holder (for an additional service provider). In the case of write operations, confidentiality is achieved with a public encipherment key which can be obtained from the ERT. The data to be written can then only be decrypted with the private decipherment key of the ERT.

### **5.3.4 Keys for authentication and confidentiality**

A vehicle may be registered for many years and during those years many other vehicles are registered or deregistered. As a consequence a registration authority has either to use always the same keys, or to use different keys for different vehicles. In order to support this latter option a key can be identified with a key identifier.

In case of encryption, the identifier of the public encipherment key is attached to the ciphertext and can then be used by a recipient to determine the corresponding private decipherment key.

For signature verification one or two public key certificates shall be appended to the signed data. For data signed by the ERT the certificate is provided by the registration authority when the private signature key is written into the ERT (see the commission ERT transaction). For data to be signed by the back office equipment the private signature key for the top level certificate is determined by means of a key identifier that can be obtained from the ERT. This key identifier and the public verification key are written into the ERT when it is manufactured.

This part of ISO/TS 24534 allows a registration authority to change its public encipherment key, the private signature key and the PIN for the ERT holder. This may e.g. be part of a periodic motor vehicle test.

**NOTE** There is no implication that the garage performing the periodic test will change this key itself. Although, it is outside the scope of this part of ISO/TS 24534 to prescribe the security measures to be applied by the registration authorities to protect their private keys, it is more likely that the garage will only establish a connection between the ERT and the registration authority; the registration authority may then securely update the ERT.

### **5.3.5 Access control to ERI data**

#### **5.3.5.1 Read access control**

##### **5.3.5.1.1 Entities with read access**

The following three types of entities may require access to ERI data

- authorities,
- authorized service providers, and
- the ERT holder.

In case the ERT has enabled encipherment capabilities, it controls read access of authorities and authorized additional service providers by means of an “access control list” that contains for each entity the following data:

- its identifier,
- its public encipherment key and key identifier, and
- an indication of whether or not this entity is an authority.

The public encipherment key is used for the encryption of a random secret key used to encrypt the ERI data sent to the ERI reader.

In case a registration authority does not support confidentiality, its public encipherment key will have a null value and any contents of the access control list will be ignored. In that case the ERI data will be sent in cleartext to the ERI reader.

##### **5.3.5.1.2 Read access for authorized authorities**

In case an ERT has enabled encipherment capabilities, a registration authority may authorize an authority for reading ERI data by writing its identifier, public encipherment key and key identifier into the access control list of the ERT (see 5.3.5.2).

The ERI reader of an authorized authority can have confidential access to the ERI data by providing the identifier of this authority. The ERT will then encrypt the ERI data with its public encipherment key.

#### 5.3.5.1.3 Read access for unauthorized authorities

An authority that is not authorized to read the ERI data shall not provide any entity identifier in its read request. The ERT will then encrypt the ERI data with the public encipherment key of the vehicle's registration authority.

Decrypting this ERI data then requires the private decipherment key of the vehicle's registration authority. This can be accomplished in several ways (which are all outside the scope of this Technical Specification):

- The ERI reader can be commissioned providing the private decipherment key of registration authority in e.g. a SAM, in which case the reader can decrypt the ERI data itself.
- The local (registration) authority may have (a SAM with) this private key and may then decrypt the ERI data obtained by the reader.
- The vehicle's registration authority may be requested to decrypt the ERI data.

NOTE Procedures for the cooperation between registration authorities are outside the scope of this Technical Specification.

#### 5.3.5.1.4 Read access for authorized service providers

Access of a service provider is controlled by adding its identifier, public encipherment key and key identifier to an access control list in the ERT. A reader of this service provider can then be commissioned with the corresponding private decipherment key (in a SAM).

When requesting the ERI data from a vehicle, the reader provides the ERT with the identifier of the service provider. If the access control list contains this identifier, the associated public encipherment key is used for the encryption of the ERI data returned to the reader. If not, the public encipherment key of vehicle's registration authority is used.

#### 5.3.5.1.5 Read access for the ERT holder

This Technical Specification provides access to cleartext ERI data if the request contains both the vehicleId and the password (PIN) supplied to the ERT holder.

Using only the VehicleId violates the requirement that the ERI shall not be easily usable for triggering an attack on the vehicle. The success of an attempt to read data using only the VehicleId as authentication information may then be used as such a trigger. The use of a PIN reduces this risk.

### 5.3.5.2 Write access control

#### 5.3.5.2.1 Entities with write access

Write access may be required by the following types of entities:

- manufacturers and registration authorities in order to customize the ERT for a particular vehicle,
- registration authorities to commission itself and to update ERI data or security data, and
- the ERT holder.

#### 5.3.5.2.2 Write access for customizing by manufacturers and registration authorities

This Technical Specification supports customizing an ERT for a particular vehicle by a manufacturer or a registration authority.

Customizing the ERT for a particular vehicle is accomplished by writing the vehicle identifier and, eventually, additional vehicle data (e.g. the registration date, registration number, engine type, etc.) into this component.

An ERT can only be customized once in its lifetime and the vehicle identifier in the ERT can then never be changed.

NOTE 1 This may be accomplished, for example, by a manufacturer during the vehicle build or by a registration authority if the ERT has to be replaced (e.g. because of a defect) or is to be retrofitted.

To obtain this write access the writing equipment shall prove that it is acting on behalf of a manufacturer or a registration authority. To this end the writing equipment shall supply one or two public key certificates:

- either a public key certificate issued either by the top-level or an intermediate certification authority, or
- in case the public key certificate is issued by an intermediate certification authority, a public key certificate for this intermediate certification authority issued by the top-level authority.

NOTE 2 As the public verification key(s) of the top-level certification authority are put into the ERT at manufacturing, this component can verify the signature on a certificate issued by the top-level certification authority.

NOTE 3 As it is only required that the data to be written into the ERT be issued by an official registration authority (and contain the correct vehicle identifier) there is no need to authorize the writing equipment. The communication channel used to exchange the ERI data from the BOE of the registration authority to the ERT may be insecure.

#### 5.3.5.2.3 Additional write access for registration authorities

In addition to customization, this Technical Specification also supports, as far as applicable, write access of a registration authority to the ERT, in order to:

- commission itself as the vehicle's registration authority;
- add or change the private signature key to be used by the ERT to sign messages and the certificate for the corresponding public verification key signed by itself;

NOTE This certificate also includes the vehicle identifier.

- add or change its public encipherment key required for the encipherment of ERI data (if confidentiality is to be supported);
- authorize other authorities by adding their identifier, public encipherment key and key identifier into the ERT's access control list (if confidentiality is to be supported);
- add or change the PIN issued to the ERT holder (if confidentiality is to be supported);

NOTE How and when a registration authority sends an ERT holder a (new) PIN is outside the scope of this Technical Specification.

- change the additional vehicle data (e.g. its registration number, its colour, its engine type, etc.) as required or allowed by local legislation.

Write access is obtained by handing over one or two public key certificates as described in the previous section.

#### 5.3.5.2.4 Write access for ERT holders

This part of ISO/TS 24534 supports write access of an ERT holder to authorize read access for

- an additional service provider by writing the identifier, public encipherment key and key identifier of this service provider into the ERT, and
- onboard applications/equipment that needs to verify or authenticate ERI data by writing the identifier, public encipherment key and key identifier into the ERT.

To obtain write access the ERT holder shall identify himself as the holder of the ERT containing the ERI data. He does so by using the vehicle identifier and a password (PIN) he has obtained from the registration authority.

NOTE How and when an ERT holder obtains this password (PIN) is outside the scope of this Technical Specification.

Using only the vehicle identifier violates the requirement that the ERI shall not be easily usable for triggering an attack on the vehicle. The acceptance of an attempt to write data using only the vehicle identifier as authentication information may then be used as such a trigger. The use of a PIN reduces this risk.

5.3.6 Public certification key identification

The top-level certification authority may use different private signature keys. A key identifier is used to determine the private signature key that corresponds to the public verification key stored in the ERT. This key identifier is stored in and can be read from the ERT.

5.4 Communication architecture description

5.4.1 Identifying a vehicle with an authorized short-range reader

Figure 5 presents the communication concept for the identification of a vehicle with an authorized ERI reader using short range communications.

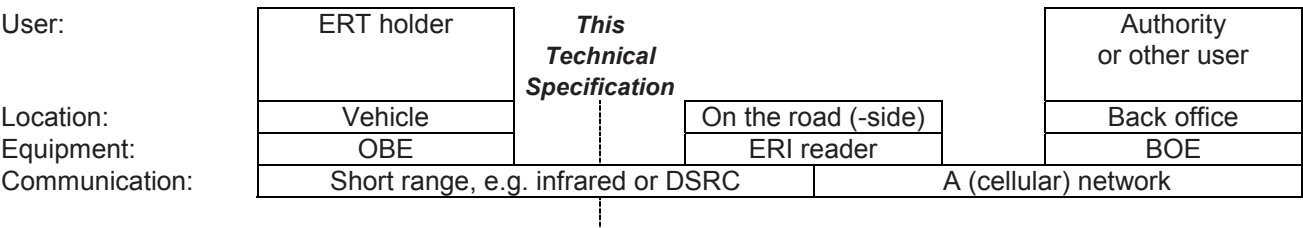


Figure 5 — Short-range communication with an authorized reader

This Technical Specification deals with the application layer of the air interface between the onboard ERI equipment and external short-range ERI readers.

NOTE The vehicle-external ERI-reader interface corresponds to the DELTA reference point, the air interface, in Annex A of ISO 14814 (see section 5.5.1 for details). The external ERI-reader-back-office interface corresponds to the ALPHA reference point in that annex.

The interface between an external ERI reader and the BOE of a back office is outside the scope of this Technical Specification. It may e.g. be used for commissioning the ERI reader, the exchange of white or black lists and/or uploading the reading results. It may e.g. be a local interface in the back office or a wide area network interface.

A back office may be an office from a (registration) authority or from an additional service provider.

A similar situation applies to, and a similar figure can be drawn for, the identification of a vehicle with an authorized external proximity reader.