TECHNICAL SPECIFICATION

ISO/TS 24534-5

First edition
2008-02-15

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

Part 5: Secure communications using symmetrical techniques

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

Partie 5: Communications sécurisées utilisant des techniques symétriques

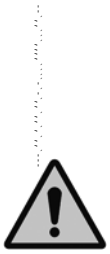
Reference number
ISO/TS 24534-5:2008(E)

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

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

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

The ERI interface defined in this part supports confidentiality measures to adhere to (inter)national privacy regulation and to prevent other misuse of electronic identification of vehicles.

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

This part of ISO/TS 24534 makes use of the basic automatic vehicle identification (AVI) provisions already defined in ISO 14814 and ISO 14816. In addition, it includes provisions for security and the use of additional registration data of a vehicle.

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

Part 5: Secure communications using symmetrical techniques

1 Scope

This Technical Specification provides the requirements for an Electronic Registration Identification (ERI) using symmetric encryption techniques that are

— based on an identifier assigned to a vehicle (e.g. for recognition by national authorities),

— suitable to be used for:

  — electronic identification of local and foreign vehicles by national authorities;

  — vehicle manufacturing, in-life maintenance and end-of-life identification (vehicle life-cycle management);

  — adaptation of vehicle data, e.g. in case of international re-sales;

  — safety related purposes;

  — crime reduction;

  — commercial services, and

— adhering to privacy and data protection regulations.

This part of ISO/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 symmetric encryption techniques.

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

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

This Technical Specification includes:

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

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

— security issues related to the communication with the ERT.

NOTE The vehicle identifiers and possible related vehicle information (as typically contained in a vehicle registration certificate) are defined in ISO/TS 24534-3, *Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 3: Vehicle data*.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

EN 12834, *Road Transport and Traffic Telematics — Dedicated Short-Range Communication (DSRC) — DSRC application layer*

3 Terms and definitions

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

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

[ISO 7498-2, definition 3.3.1]

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

[ISO 7498-2, definition 3.3.2]

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

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

[ISO 7498-2, definition 3.3.4]

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

[ISO 7498-2, definition 3.3.10]

3.7
challenge
data item chosen at random and sent by the **verifier** to the claimant, which is used by the **claimant**, in conjunction with secret information held by the **claimant**, to generate a response which is sent to the **verifier**

[ISO 9798-1, definition 3.3.5]

3.8
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]

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

[ISO/IEC 10181-2]

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

[ISO 7498-2]

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

[ISO 7498-2]

3.12
data integrity
integrity
property that data has not been altered or destroyed in an unauthorized manner [ISO7498-2]

3.13
decipherment
decryption
reversal of a corresponding reversible **encipherment**

[ISO 7498-2, definition 3.10]

3.14
distinguishing identifier
information which unambiguously distinguishes an entity

[ISO 9798-1, definition 3.3.9]

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

3.16
electronic registration reader
ERR
a 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 as a relay in the exchange of ERI data protocol units between an ERT and an ERI reader/writer.

3.17
electronic registration tag
ERT
the 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 SAM (secure application module).

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

3.18
encipherment
encryption
the cryptographic transformation of data to produce ciphertext

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

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

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

[ISO 7498-2, definition 3.3.29]

3.20
entity authentication
corroboration that an entity is the one claimed

[ISO 9798-1, definition 3.3.11]

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

[ISO 24534-3, definition 3.4]

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

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

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

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

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

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

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

3.25
external ERI reader
ERI reader 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).

3.26
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).

3.27
identification
action or act of establishing the identity

NOTE See also vehicle identification.

3.28
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]

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

[ISO 14815, definition 4.8]

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

[ISO 7498-2, definition 3.3.35]

3.31
masquerade
pretence by an entity to be a different entity

[ISO 7498-2, definition 3.3.36]

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

[ISO 9798-1, definition 3.3.14]

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

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

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

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

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

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

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

[ISO 7498-2, definition 3.3.38]

3.37
principal
entity whose identity can be authenticated

[ISO/IEC 10181-2, definition 3.15]

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

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

[ISO 7498-2, definition 3.3.43]

3.39
random number
time-variant parameter whose value is unpredictable

[ISO 9798-1, definition 3.3.24]

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

NOTE It is expected that the registration authority with respect to the ERI data may be the same authority that keeps the official register in which the vehicle and is owner or lessee are listed. This is, however, not required by this Technical Specification.

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

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

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

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

3.42
security
protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them

[ISO 12207, definition 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.

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

[ISO/IEC 10181-1, definition 3.3.17]

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

NOTE Adapted from ISO/IEC 10181-1, definition 3.3.20.

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

[ISO 7498-2, definition 3.3.51]

3.46
sequence number
time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

[ISO 9798-1, definition 3.3.27]

3.47
system operator
organization responsible for the operation of the system

NOTE For this part of ISO/TS 24534, a system operator also acts as the registration authority and the security authority in his jurisdiction.

3.48
system operator key
access key for a system operator

3.49
threat
potential violation of security

[ISO 7498-2, definition 3.3.55]

3.50
vehicle identification
action or act of establishing the identity of a vehicle

3.51
verifier
entity which is or represents the entity requiring an authenticated identity

NOTE 1 A verifier includes the functions necessary for engaging in authentication exchanges.

NOTE 2 Adapted from ISO/IEC 10181-2, definition 3.20.

4 Symbols and abbreviations

AEI Automatic Equipment Identification

AES Advanced Encryption Standard

ASN.1 Abstract Syntax Notation One (as defined in ISO 8824)

AVI Automatic Vehicle Identification

BOE Back Office Equipment

DES Data Encryption Standard

EN Europäische Norm (German), English: European Standard

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

ERI Electronic Registration Identification

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

ERT Electronic Registration Tag

EU European Union

IEC International Electrotechnical Commission

ISO International Organization for Standardization

OBE OnBoard Equipment

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

PICS Protocol Implementation Conformance Statement(s)

PIN Personal Identification Number

SAM Secure Application Module

Triple-DES Triple-Data Encryption Standard

VIN Vehicle Identification Number

5 System communications concept

5.1 General

Clause 5 is informative only.

This clause provides an introduction of 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 interfaces are provided in Clause 6 and Annex A. Annex C contains a form to specify the limitations of an actual communication protocol implementation.

This clause only deals with interfaces using symmetric encryption techniques. Symmetric encryption techniques are based on secret keys that are shared by a community of one or more users. Such a community is essentially a closed user group in which it is trusted that secret keys are not revealed to outsiders.

It is assumed that the users of the closed user group are all operating within the jurisdiction of one ERI system operator responsible for key management and acting as the registration authority in his jurisdiction.

A more generic interface based on asymmetric techniques, with various (security) capability levels and supporting cooperation between multiple (registration) authorities (i.e. multiple security domains) is defined in ISO/TS 24534-4.

5.2 Overview

5.2.1 Vehicle registration identification

ERI, Electronic Registration Identification, is the action or act of identifying a vehicle with electronic means for purposes as mentioned in the scope of this part Technical Specification.

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

NOTE The preferred vehicle identifier is the VIN that is assigned to the vehicle by its manufacturer in accordance to ISO 3779 but alternatives are supported as well. See ISO/TS 24534-3, *Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 3: Vehicle data*, for details about the vehicle identifier and additional vehicle data.

In this Technical Specification, 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 specified in this part of Technical Specification.

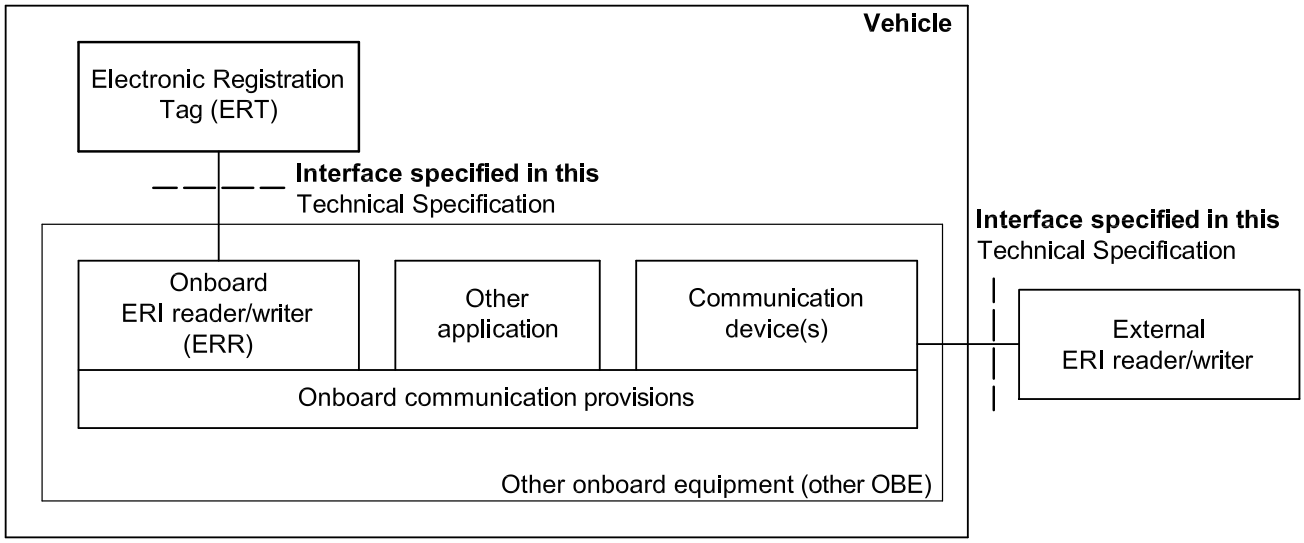


Figure 1 — System concept and supported interfaces

The onboard component that provides a secure environment for the ERI data and security data is called the electronic registration tag (ERT).

NOTE An implementer may integrate other provisions into the ERT, as long as this does not compromise the security of the ERT.

An ERT operates in one of two modes:

— Non-commissioned mode,
when the ERT contains no system operator keys.
When operating in the non-commissioned mode, the authentication phase (see below) is not supported and the only operation allowed is to commission the ERT.

— Commissioned mode,
when a system operator has written its keys into the ERT.
When operating in the commissioned mode the authentication phase (see below) is supported.

A system operator may also decommission an ERT, i.e. delete all key from the ERT. The ERT then returns to its non-commissioned mode and the only operation allowed is again to commission the ERT.

An ERT is tailored to a specific vehicle in one or more steps:

— First, the ERT is customized with the vehicle identifier and, optionally, additional ERI data.
This step can only be performed once in the lifetime of an ERT.

— Next, the system operator may register changes of the additional ERI data (i.e. the ERI data with the exception of the vehicle identifier).

ERI data may only be written/updated in commissioned mode and only by the system operator.

It is assumed that all ERT and all onboard and external readers and writers will be part of the same security domain, i.e. within the jurisdiction of one single ERI system operator responsible for the security policy and its implementation.

It is also assumed that the system operator is also acting as the registration authority in their jurisdiction.

NOTE 1 In order to accommodate the needs of different system operators, different selections of additional ERI data can be included in an ERT (see ISO 24534-3 for details).

The onboard communication provisions shall be capable to transfer data from or to the ERT without modifying that data.

NOTE 2 The onboard communication provisions may e.g. be part of an onboard platform for transport applications.

A communication device may communicate with a short-range ERI reader/writer or remote with back office equipment (BOE).

A onboard communication device external to the ERT 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 Technical Specification, the following “roles” for natural or legal persons are distinguished.

a) A system operator, who is responsible for the operation of the ERI system. An ERI system operator is also the security authority for the ERI security domain and responsible for generating secret keys to be used for authentication. A system operator also acts as the registration authority, i.e. as the authority for writing vehicle-related data into the ERT.

   NOTE 1 It is expected that the registration authority with respect to the ERI data is the same authority that keeps the register in which the vehicle is listed. This is, however, not required by this Technical Specification.

   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).

b) Authorities, who are entitled (e.g. by the virtue of public legislation) and authorized by the system operator to read the ERI data and encrypted access control list entries from a vehicle.

   NOTE 3 Roles and requirements related to the specification, design and manufacturing (including testing) of an ERT are outside the scope of this part of this Technical Specification.

5.2.4 The communications context for reading

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

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

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.

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.

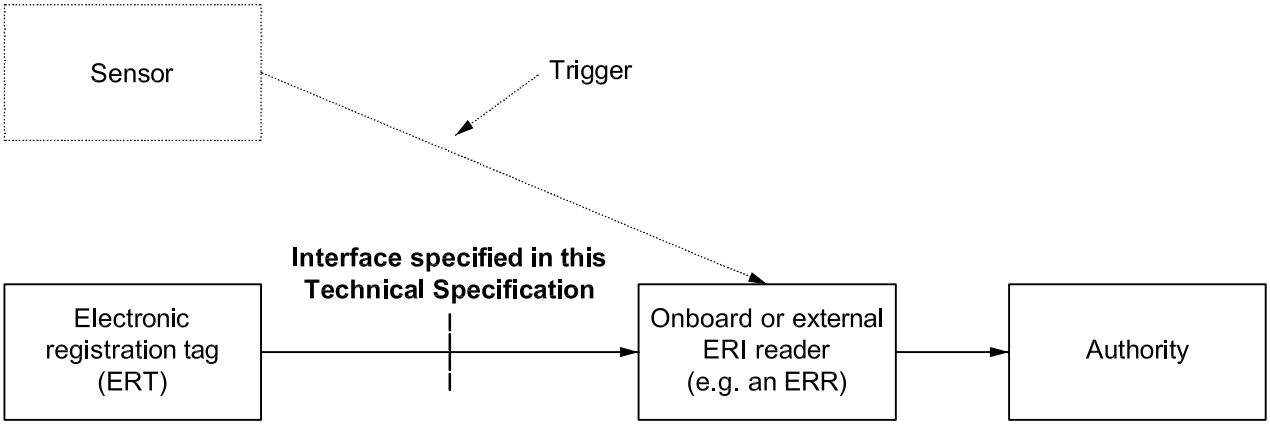


Figure 2 — Communication context for reading from an ERT

The equipment used by an entity in an 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 communicates either directly or indirectly with the ERT: directly in case of a hand-held reader 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.

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.

The distribution of functions between BOE and an external ERI writer is outside the scope of this Technical Specification. A system operator 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.

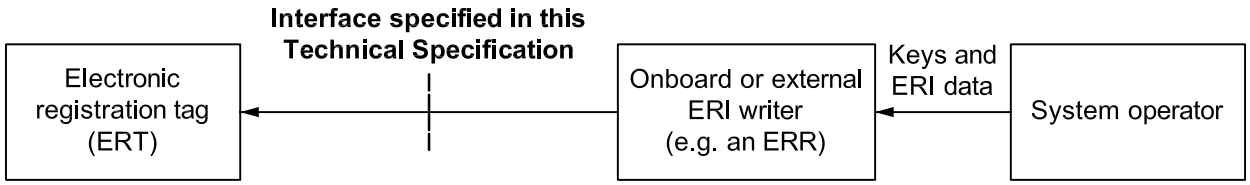


Figure 3 — Communication context for writing into an ERT

5.2.6 Service levels supported

This part of ISO/TS 24534 supports a secure communication with an ERT within one jurisdiction based on symmetric encryption techniques.

A more generic interface based on asymmetric techniques, with various (security) capability levels and supporting cooperation between multiple (registration) authorities (i.e. security domains) is defined in ISO/TS 24534-4.

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.

a) The use of an ERT may be mandatory and, therefore, should be fraud resistant. Using ISO 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).

b) A reading of an ERT should be suitable as legal evidence.

c) 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); consequently, an ERT should also be resistant against passive threats.

d) ERI shall have the capability to provide protection measures to prevent ERI from being used to trigger an attack on a vehicle.

e) The performance of security mechanisms must be achievable within the time available for communications whilst the vehicle is moving.

EXAMPLE Reading a vehicle at 180 km/h within a 10 m 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 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).

d) The ERI data is correctly read from the ERT (data integrity, manipulation detection). This is achieved by standard mechanisms used in data communications 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. This is achieved by encrypting the ERI data together with a challenge code provided by the ERI reader.

NOTE 1 This part of ISO/TS 24534 only deals with c), d), and e). The items a) and b) are specified in ISO/TS 24534-2, *Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 2: Operational requirements.*

NOTE 2 Using technical (ISO/IEC 9798-2) terminology, c) and e) are supported using a three pass mutual authentication mechanism with unidirectional keys. Uniqueness/timeliness is controlled by generating and checking random numbers and sequence numbers.

5.3.3 Confidentiality while reading ERI data

This Technical Specification supports confidentiality by delivering ERI data in ciphertext. 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 or random number may be added to the ERI data before encryption.

Confidentiality is only required for reading ERI data from an ERT, not for writing data into an ERT.

5.3.4 Keys for authentication and confidentiality

The same secret key is used for both authentication and confidentiality.

A vehicle may be registered for many years and during those years many other vehicles are registered and deregistered. As a consequence, a system operator 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 and both an ERT as well as an ERI reader/writer may use multiple keys.

In order to allow ERT with one or multiple keys to be interoperable with ERI readers/writers with one or multiple keys, the following procedure is used.

a) In case an ERI reader/writer wants to select an ERT key, it sends the ERT list a key numbers form which the ERT may select one to be used for its responses.

b) In case an ERT has one of the requested keys, it uses one of them. If an ERT does not contain a requested key but has one or more other keys, it may choose any key it has for its responses. If the ERT does not (yet) contain any key, it simply does not use any key.

c) In case an ERT wants to select an ERI reader/writer key, it sends the reader/writer a list of key numbers to choose from for its responses.

d) In case an ERI reader/writer has one of the requested keys, it uses one of them. If not, the reader/writer uses for its responses the same key as used by the ERT its request.

5.3.5 Access control to ERI data

There is no access control unless at least one key is loaded into the ERT.

If one or more keys are loaded into an ERT, access control is based on a mutual authentication procedure using unidirectional secret keys.

There are two groups of keys: one for system operators and one for authorities.

A system operator key provides full read/write access to both the ERI data and the security data.

An authority key only provides read access to:

a) The ERI data: the vehicle identifier and the additional vehicle data;

b) The historical data, if available;

c) Access control list entries (see below) in ciphertext that can be decrypted by the system operator.

5.4 Communication architecture description

5.4.1 Overall communication concept for identifying vehicles

Figure 4 presents the communication concept for the identification of a vehicle.

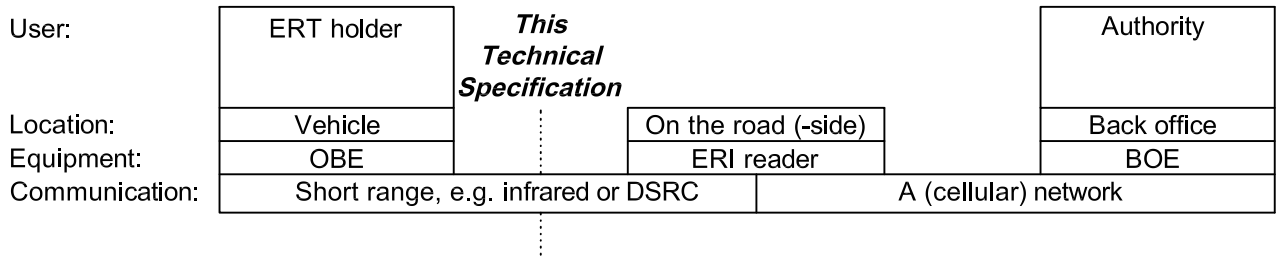


Figure 4 — Overall local communication concept for identification

This Technical Specification deals with the air interface between the onboard ERI equipment in a vehicle and a short-range external ERI reader.

NOTE The vehicle–external ERI-reader interface corresponds to the DELTA reference point, the air interface, in the informative Annex A of ISO 14814, see 5.5.1 for details. The external ERI-reader–back-office interface corresponds to the ALPHA reference point in this 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.

5.4.2 Overall communication concept for remote access

This part of ISO/TS 24534 also supports remote access to an ERT. A system operator may e.g. use remote access, if implemented, to check or update the additional ERI data or the security data.

Figure 5 presents the communication concept for remote access to a vehicle's ERT.

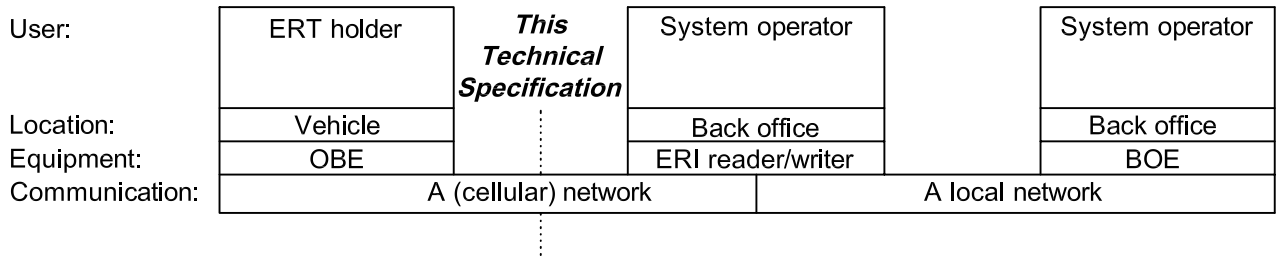


Figure 5 — Overall communication concept for remote access

This Technical Specification deals with the network interface between the onboard ERI equipment in a vehicle and a remote external ERI reader/writer.

NOTE Whether or not remote access capabilities are implemented is outside the scope of this Technical Specification.

5.4.3 The onboard communication

Figure 6 presents an abstract overview of a possible onboard communication architecture.

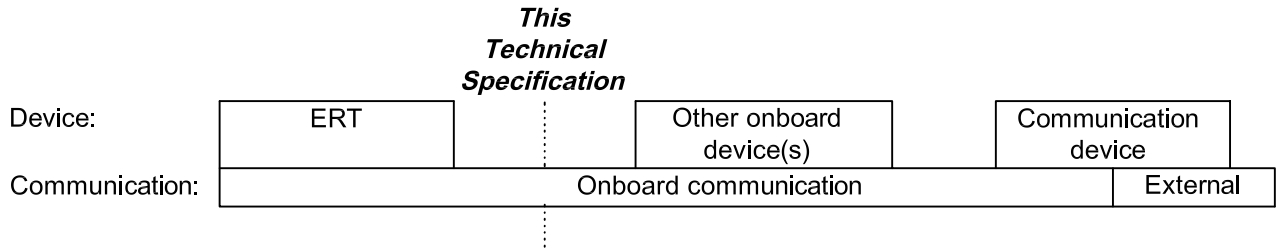


Figure 6 — The onboard architecture

NOTE Figure 6 does not imply that the ERT and the communication device shall be separate components. This may or may not be the case for a specific implementation.

5.5 Interfaces

5.5.1 The short-range air interface

The communication between the onboard ERI equipment and a short-range external ERI reader/writer uses the protocol stack as shown in Figure 7.

AVI layer (conform to ISO 14816 plus additional services)
ERI layer (adding ERI security and management services)
An application layer, e.g. the DSRC application layer (conform to ISO 15628 or EN 12834) or a similar layer
Lower layers

Figure 7 — Protocol stack air interface

The relation between these layers and the reference points BETA to ZETA in the informative Annex A of ISO 14814 is depicted in Figure 8: (reference point ALPHA is located between the ERI reader and the BOE of a back office).

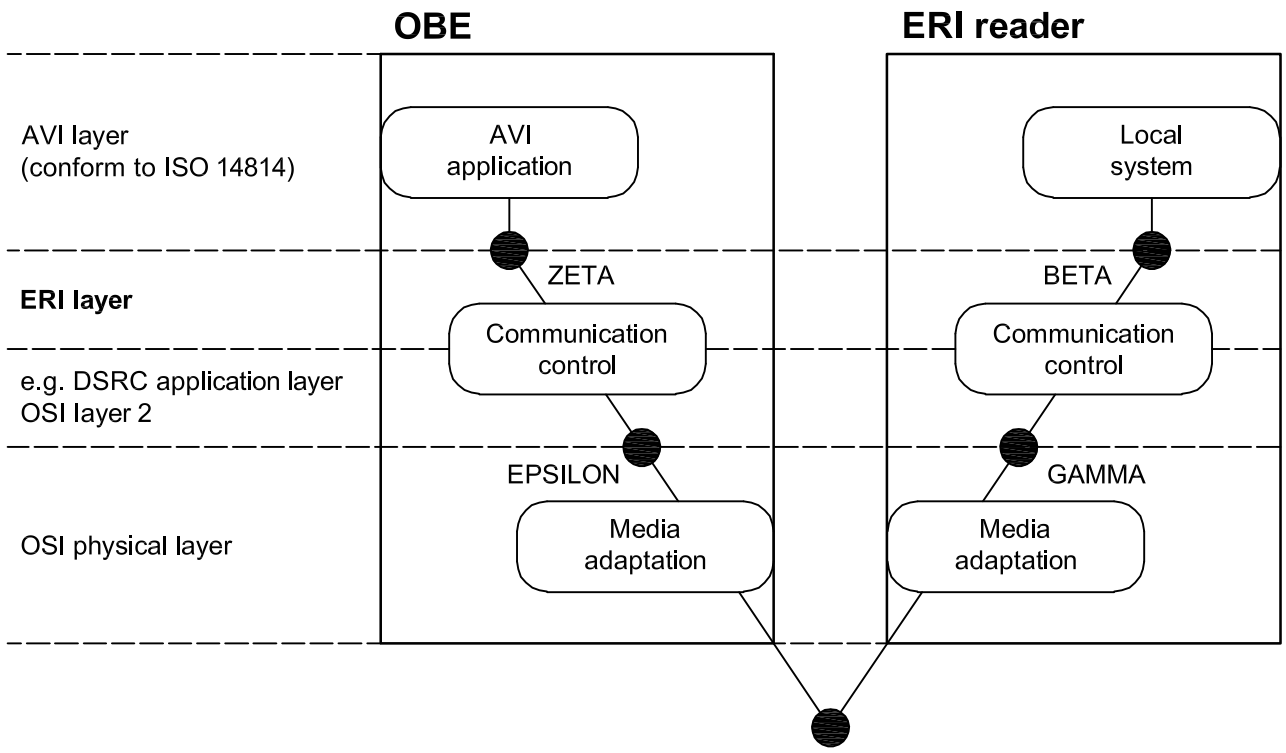


Figure 8 — The location of the ERI layer in the ISO 14814 reference architecture

5.5.2 The onboard interface with the ERT

The communication between an ERT and an onboard ERI reader/writer uses the protocol stack as shown in Figure 9.

AVI layer (conform to ISO 14816 plus additional services)
ERI layer (adding ERI security and management services)
A transmission layer, e.g. ISO 14443
Lower layers, e.g. ISO 14443, ISO 15693, etc.

Figure 9 — Protocol stack ERT interface

6 Interface requirements

6.1 Overview

Clause 6 defines the interface to access the ERI data in the ERT and contains the following subclauses:

— 6.2 provides an abstract definition;

— 6.3 defines the onboard interface with the ERT;

— 6.4 defines the short-range air interface between the onboard ERI equipment and an external ERI reader/writer;

— 6.5 defines the interface for remote access.

The onboard interface is defined as an implementation of the abstract definitions in 6.2.

The external interfaces as defined in 6.4 and 6.5 are either used to communicate directly with the ERT in case the onboard communication provisions are integrated into the ERT, or used indirectly to relay the ERI protocol data units to the onboard ERI reader/writer. (See Figure 1).

6.2 Abstract transaction definitions

6.2.1 Transaction overview

Table 1 defines the ERT transactions.

Table 1 — Required and optional transactions

Subclause	Transaction	Req	Description
6.2.4	mutualAuthenticate1	R	Required for mutual authentication
6.2.5	mutualAuthenticate2	R	Required for mutual authentication
6.2.6	getSecretKeyEriData	R	For ERI by authorities or system operator
6.2.7	setSecretKeyEriData	R	For customizing an ERT and updating additional ERI data by a system operator
6.2.8	commissionSecretKeyErt	A, C	For a system operator to load his symmetric key data into an ERT
6.2.9	decommissionSecretKeyErt	O	To remove the system operator keys
6.2.10	updateAccessControlList	A, C	To add or remove authorities to or from the access control list of an ERT
6.2.11	getCiphertextAccessControlListEntry	O	To retrieve the entries of the access control list in cipher text by an authority or system operator
6.2.12	endOfSession	R	To indicate the end of an ERI session

NOTE The column headed “Req” indicates whether a transaction is always required (R), required for confidentiality (C), required for authentication (A) or being optional (O).

6.2.2 Session phases

The communication with an ERT is session oriented. A complete session consists of the following consecutive phases.

a) The mutual authentication phase, that provides for the mutual authentication of an ERI reader/writer and an ERT if the ERT is in commissioned mode. In this phase, the mutualAuthenticate1 and mutualAuthenticate2 transactions are consecutively invoked and performed. In case the ERT is in non-commissioned mode, the mutual authentication phase is skipped.

b) The data exchange phase, that starts directly for an ER in non-commissioned mode and for an ERT is commissioned mode after a successful mutual authentication. In the data exchange phase, ERI data or security data is exchanged between the ERI reader/writer and ERT. During this phase, data exchange transactions may be invoked in any order.

c) The session release phase which terminates the session.

In case of any error and unless specified otherwise, the session shall terminate without further notice.

6.2.3 ERI transactions and protocol data units

6.2.3.1 The transaction concept

Writing and reading data to or from an ERT shall be achieved by means of transactions which are defined as instances of the TRANSACTION information object class.

The TRANSACTION information object class is defined as follows:

```
TRANSACTION ::= CLASS {
        &ArgumentType                   ,
        &ResultType                     ,
        &transactionCode                INTEGER UNIQUE
        }
WITH SYNTAX {
        ARGUMENT                        &ArgumentType
        RESULT                          &ResultType
        CODE                            &transactionCode
        }
```

A transaction shall be invoked by an ERI reader, an ERI writer and shall be performed by the ERT.

No transaction shall be invoked by an onboard ERT reader/writer while the ERT is still performing another transaction.

The &ArgumentType field shall specify the data type of the argument of the transaction. If omitted, then the transaction takes no argument value.

The &ResultType field shall specify the data type of the value returned with the result of the transaction.

The &transactionCode field specifies the integer value which is used to identify the transaction, e.g. when it is to be invoked.

6.2.3.2 ERI protocol data units

The ERI protocol data units (PDUs) are defined as follows:

```
SecretKeyEriPdu ::= CHOICE {
        requestPdu                      SecretKeyEriReqPdu,
        reponsePdu                      SecretKeyEriRspPdu
        }

SecretKeyEriReqPdu ::= SEQUENCE {
        transactCode                    TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
        argument                        TRANSACTION.&ArgumentType
                                        ({SecretKeyEriTransactions} {@.transactCode}) OPTIONAL
        }

SecretKeyEriRspPdu ::= SEQUENCE {
        transactCode                    TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
        result                          TRANSACTION.&ResultType
         ({SecretKeyEriTransactions} {@.transactCode})
        }

SecretKeyEriTransactions TRANSACTION ::= { mutualAuthentication1 | mutualAuthentication2 |
        getSecretKeyEriData | setSecretKeyEriData |
        commisionSecretKeyErt | decommisionSecretKeyErt |
        updateAccessControlList | getCipertextAccessControlListEntry | endOfSession
        }
```

A secret key ERI data protocol unit is of type SecretKeyEriPdu and either a SecretKeyEriReqPdu or a SecretKeyEriRspPdu.

The SecretKeyEriReqPdu data protocol unit shall be used for the invocation of a transaction to be performed by the ERT.

The SecretKeyEriRspPdu data protocol unit shall be used for the result of a transaction performed by the ERT.

SecretKeyEriTransactions specifies the set of ERI transactions (see the subclauses below for details).

The transactCode component shall contain the value of the transaction code for a transaction in the set EriTransactions.

The argument component, if present, shall be of the same type as specified for the argument of the transaction identified by the value of transactCode.

The argument component shall be present if the argument for the transaction is defined and absent if not.

The result component shall be of the same type as specified for the result of the transaction identified by the value of transactCode.

6.2.4 Mutual authentication 1

6.2.4.1 Service definition

The mutualAuthentication1 transaction is the first transaction to be used in the mutual authentication phase.

The mutualAuthentication1 transaction is invoked by an ERI reader/writer and performed by an ERT operating in commissioned mode.

If the ERT operates in non-commissioned mode, i.e. does not yet contain any key, the transaction is ignored and no response is produced.

The transaction is used by the invoking ERI reader/writer to authenticate an ERT and used by this ERT to initiate the authentication of the invoking ERI reader/writer.

6.2.4.2 Protocol specification

The mutual authentication transaction is defined as follows:

```
mutualAuthentication1 TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        1
        }
```

An OCTET STRING is used for both the argument and the result of the transaction.

6.2.5 Mutual authentication 2

6.2.5.1 Service definition

The mutualAuthentication2 transaction is the second and last transaction to be used in the mutual authentication phase.

The mutualAuthentication2 transaction is invoked by an ERI reader/writer after it received a satisfactory response on its mutualAuthentication1 transaction.

A response on a mutualAuthentication1 transaction is only satisfactory if it contains the ERT challenge encrypted with a correct secret key.

The transaction is used by the invoking ERI reader/writer to signal the ERT that it has accepted the ERT authentication and to respond on the authentication request from the ERT.

The mutualAuthentication2 transaction is performed by the ERT and a response is only sent if the request from the ERI reader/writer was satisfactory. If not, the ERT does not send a response.

A request from an ERI reader/writer is only satisfactory if it contains the reader/writer challenge encrypted with a correct secret key.

6.2.5.2 Protocol specification

The mutual authentication transaction is defined as follows:

```
mutualAuthentication2 TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        2
        }
```

An OCTET STRING is used for both the argument and the result of the transaction.

6.2.6 Get secret key ERI data

6.2.6.1 Service definition

The get secret key ERI data transaction shall be used to obtain ERI data from an ERT.

The get secret key ERI data transaction shall only be invoked in the data exchange phase and shall only be performed by the ERT when it is customized and in the commissioned mode.

In case the transaction is not invoked in the data exchange phase or when the ERT is not customized or in the non-commissioned mode, the invocation shall be ignored, the transaction shall not be performed and no result will be produced.

Table 2 — Get secret key ERI data transaction parameters

Parameter	Request	Response	Remark
Argument	O		In cleartext or ciphertext
ERI data		M	In cleartextciphertext
NOTE M: The parameter is mandatory. O: The parameter is optional.			

6.2.6.2 The request primitive

The request contains the operation to be written into the ERT in cleartext or in ciphertext.

6.2.6.3 The response primitive

The response comprises the ERI data as stored into the ERT cleartext or in ciphertext.

6.2.6.4 Protocol specification

The get secret key ERI data transaction is defined as follows:

```
getSecretKeyEriData TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        3
        }
```

An OCTET STRING is used for both the argument and the encrypted result of the transaction.

6.2.7 Set secret key ERI data

6.2.7.1 Service definition

The set secret key ERI data transaction shall be used to write the ERI data into an ERT.

The set secret key ERI data transaction shall only be invoked in the data exchange phase and shall only be performed by the ERT when it is in the commissioned mode.

In case the transaction is not invoked in the data exchange phase or when the ERT is in the non-commissioned mode, the invocation shall be ignored, the transaction shall not be performed and no result will be produced.

Table 3 — Set secret key ERI data transaction parameters

Parameter	Request	Response	Remark
ERI data	M		In cleartext or in ciphertext
Result		M	
NOTE M: The parameter is mandatory.			

6.2.7.2 The request primitive

The request contains the ERI data to be written into the ERT in cleartext or in ciphertext.

The new ERI data will completely replace the old ERI data.

6.2.7.3 The response primitive

The response is used to indicate the result of the set transaction.

6.2.7.4 Protocol specification

The set secret key ERI data transaction is defined as follows:

```
setSecretKeyEriData TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        4
        }
```

An OCTET STRING is used for both the argument and the result of the transaction.

6.2.8 Commissioning secret key ERT

6.2.8.1 Service definition

The commissioning transaction shall be used for commissioning the ERT or to update the ERT security parameters.

The security data entered or updated with this transaction consists of the access keys for the system operator and the key identifiers associated with these keys.

The commissioning transaction shall only be used in the data exchange phase.

In case the transaction is not invoked in the data exchange phase the invocation shall be ignored, the transaction shall not be performed and no result will be produced.

After the transaction is successfully performed by an ERT, the ERT is in commissioned mode.

Table 4 — Commissioning secret key ERT transaction parameters

Parameter	Request	Response	Remark
Commission data	M		In cleartext or in ciphertext
Result		M	
NOTE M: The parameter is mandatory.			

6.2.8.2 The request primitive

The request contains the security data to be written into the ERT in ciphertext.

The new security data will completely replace the old ERI data.

6.2.8.3 The response primitive

The response is used to indicate the result of the commissioning transaction.

6.2.8.4 Protocol specification

The commissioning secret key ERT transaction is defined as follows:

```
commissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        5
        }
```

An OCTET STRING is used for both the argument and the result of the transaction.

6.2.9 Decommissioning secret key ERT

6.2.9.1 Service definition

The decommissioning transaction shall be used for decommissioning the ERT, i.e. to remove the ERT security parameters and access control list.

The decommissioning transaction shall only be used in the data exchange phase.

In case the transaction is not invoked in the data exchange phase, the invocation shall be ignored, the transaction shall not be performed and no result will be produced.

After the transaction is successfully performed by an ERT the ERT is in non-commissioned mode.

Table 5 — Decommissioning secret key ERT transaction parameters

Parameter	Request	Response	Remark
Argument			
Result			
NOTE Blank: The parameter is not used.			

6.2.9.2 The request primitive

The request contains no data.

6.2.9.3 The response primitive

The response contains no data.

6.2.9.4 Protocol specification

The decommissioning secret key ERT transaction is defined as follows:

```
decommissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT                NULL
        RESULT                  NULL
        CODE                    6
        }
```

A NULL value is used for both the argument and the result of the transaction.

6.2.10 Update access control list

6.2.10.1 Service definition

The updateAccessControlList transaction shall be used to add or delete entries to the access control list of the ERT.

The access control list contains the keys and their associated key identifiers for authorities.

The transaction shall only be invoked in the data exchange phase and shall only be performed by the ERT when it is in the commissioned mode.

In case the transaction is not invoked in the data exchange phase or when the ERT is in the non-commissioned mode, the invocation shall be ignored, the transaction shall not be performed and no result will be produced.

Table 6 — Update access control list transaction parameters

Parameter	Request	Response	Remark
Argument	M		In ciphertext
Result		M	
NOTE M: The parameter is mandatory.			

6.2.10.2 The request primitive

In case a key is added, the request contains an access key for an authority and its associated key identifier.

In case a key is added and the access control list already contains a key with the same key identifier, the old key is replaced with the new one.

In case a key shall be deleted, the request contains the key identifier associated with that key.

6.2.10.3 The response primitive

The response is used to indicate the result of the update access control list transaction.

6.2.10.4 Protocol specification

The updateAccessControlList transaction is defined as follows:

```
updateAccessControlList TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        7
        }
```

An OCTET STRING is used for both the argument and the result of the transaction.

6.2.11 Get ciphertext access control list entry

6.2.11.1 Service definition

The getCiphertextAccessControlListEntry transaction shall be used to retrieve an access control list entry from the access control list in ciphertext from the ERT.

The transaction shall only be invoked in the data exchange phase and shall only be performed by the ERT when it is in the commissioned mode.

In case the transaction is not invoked in the data exchange phase or when the ERT is in the non-commissioned mode, the invocation shall be ignored, the transaction shall not be performed and no result will be produced.

Table 7 — Get ciphertext access control list entry transaction parameters

Parameter	Request	Response	Remark
Argument	M		In ciphertext
Result		M	
NOTE M: The parameter is mandatory.			

6.2.11.2 The request primitive

The request contains the number of the entry of the access control list from which the key and its associated key identifier shall be returned.

6.2.11.3 The response primitive

The response shall contain the key and its associated key identifier form the entry in the access control list as indicated in the request.

6.2.11.4 Protocol specification

The getCiphertextAccessControlListEntry transaction is defined as follows:

```
getCiphertextAccessControlListEntry TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        8
        }
```

An OCTET STRING is used for both the argument and the result of the transaction.

6.2.12 End of Session

6.2.12.1 Service definition

The end of session transaction shall be used to signal the end of a session.

The end of session transaction shall only be invoked in the data exchange phase and once invoked, the session enters the “session release phase”.

Table 8 — End of session transaction parameters

Parameter	Request	Response	Remark
Argument	O		In cleartext or in ciphertext
NOTE O: The parameter is optional.			

6.2.12.2 The request primitive

The request contains the operation to be written into the ERT in cleartext or in ciphertext, and it is used to signal the end of the session between an ERT and an ERI reader/writer.

6.2.12.3 The response primitive

The response does not carry any value. It is only used to confirm the end of a session.

6.2.12.4 Protocol specification

The end of session transaction is defined as follows:

```
endOfSession TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      NULL
        CODE                        9
        }
```

The transaction uses an OCTET STRING for argument and a NULL value for its result.

6.3 The onboard interface to the ERT

6.3.1 General ERT interface requirements

The ERI data and chip identifier can only be accessed as specified in this part of ISO/TS 24534.

An application layer protocol data units to be exchanged with an ERT shall be an ERI protocol data unit of type SecretKeyEriPdu, i.e. of type SecretKeyEriReqPdu or of type SecretKeyEriRspPdu.

An ERI protocol data unit shall be encoded conforming to the canonical Packed Encoding Rules (PER) (CANONICAL-PER) ALIGNED variant as defined in ISO 8825-2.

The lower layer protocols (session and lower, as applicable) shall comply with international standards.

NOTE 1 If required, an ERI protocol data unit may be segmented and reassembled (in ISO/IEC 7498-1 terminology) as appropriate.

NOTE 2 Collisions between an onboard reader or writer and a (hand held) reader or writer are not expected. If necessary, the other onboard ERI equipment should be switched off when a hand-held ERI reader or writer is used.

6.3.2 An ISO 14443 interface

In case the interface with an ERT is based on ISO 14443, the interface between an ERT and an onboard ERI reader/writer shall comply with ISO 14443 (all parts), with:

— The ERT acting as a PICC (proximity integrated circuit card) of type A or B;

— The onboard ERI reader/writer acting as a PCD (proximity coupling device) supporting both type A and B.

An ERI protocol data unit shall be directly transferred using the INF field of one of more I-blocks (see ISO 14443-4).

An ERI protocol data unit shall not be packed into ISO 7816-4 application protocol data units as suggested in ISO 14443-4.

Segmenting and reassembling of an ERI protocol data unit shall be accomplished, if required, with chaining, as specified in ISO 14443-4.

6.4 The short-range air interface

6.4.1 General short-range air interface requirements

A short-range air interface shall be capable of exchanging ERI data protocol units of type SecretKeyEriPdu and encoded conform the canonical PER rules (CANONICAL-PER) ALIGNED variant as defined in [ISO 8825-2].

The lower layer protocols (session and lower as applicable) shall comply with international standards.

NOTE If required, an ERI protocol data unit can be segmented and reassembled (in ISO/IEC 7498-1 terminology) as appropriate.

6.4.2 The use of the DRSC application layer protocol

6.4.2.1 General

If the DSRC application layer protocol is used for ERI transactions, ISO 15628 (or EN 12834 within the EU) shall be applied as specified in this Clause.

NOTE This makes the ERI DSRC interface compatible with other DSRC application interfaces like, for example, that defined in ISO 14906 [15].

6.4.2.2 Use of the DSRC initialization service

Whenever a DSRC link is to be used for ERI transactions, the ISO 15628/EN 12834 initialization service shall be used as follows:

a) either the mandApplications component or the nonmandApplications component of the initialization-request T-PDU (beacon service table, BST) shall contain an ERI application component:

b) the applications component of the initialization-response T-PDU (vehicle service table, VST) shall contain an ERI application component.

c) The value of the ERI application component in an initialization-request or an initialization-response shall be as follows:

   1) the aid component shall have the value 'automatic-vehicle-identification'.

   2) the eid component may be omitted and, if present, shall be ignored by the ERI application.

   3) the parameter component may be omitted or may contain the necessary data (e.g. authentication data).

NOTE 1 The designation of an application as mandatory or non-mandatory and its position in the list of applications is outside the scope of this standard. It only influences the priority of the ERI application relative to other applications identified in the BST (see ISO 15628, 7.3.2.2/EN 12834, 7.3.2).

NOTE 2 The eid component and the parameter component may however be used for other, non ERI, AVI applications.

6.4.2.3 Use of the DSRC action request

An ERI transaction request is sent from an ERI reader/writer to the onboard DRSC unit as an ISO 15628/EN 12834 action-request as follows:

a) the value of the mode component shall be TRUE (as all ERI transactions are confirmed);

b) the value of the eid component shall be 0;

c) the value of the actionType component shall be secretKeyEriTransaction <<to be registered with NEN>>;

d) the accessCredentials component shall not be present;

e) the value of the accessParameter component shall be passed as received to the ERT as the value of an secretKeyEriReqPdu;

f) the iid component shall not be present.

NOTE The action-request shall be of type Action-Request which is defined in ISO 15628/EN 12834 as follows:

```
Action-Request ::= SEQUENCE {
        mode                    BOOLEAN,
        eid                     Dsrc-EID,
        action                  Type ActionType,
        accessCredentials       OCTET STRING (SIZE (0..127,...)) OPTIONAL,
        actionParameter         Container OPTIONAL,
        iid                     Dsrc-EID OPTIONAL
        }
```

(end of note)

6.4.2.4 Use of the DSRC action response

A ERI transaction response received from an ERT is sent by the onboard DRSC unit to the external ERI reader as an ISO 15628/EN 12834 action-response as follows:

a) the value of the eid component shall be 0;

b) the iid component shall not be present;

c) the value of the responseParameter component shall be the value of the secretKeyEriRspPdu as received from the ERT;

d) the ret component may be omitted and, if present, shall be ignored when the secretKeyEriRspPdu is also present.

NOTE The action-response shall be of type Action-Response which is defined in ISO 15628/EN 12834 as follows:

```
Action-Response ::= SEQUENCE {
        Fill                    BIT STRING (SIZE(1)),
        eid                     Dsrc-EID,
        iid                     Dsrc-EID OPTIONAL,
        responseParameter       Container OPTIONAL,
        ret                     ReturnStatus OPTIONAL
        }
```

(end of note)

In case the DSRC device is not capable of transferring an secretKeyEriReqPdu to an ERT an ISO 15628/EN 12834 action-response containing a ret component of type ReturnStatus is returned to the roadside unit.

NOTE The mechanisms to be used for passing an SecretKeyEriReqPdu from a DRSC device to the ERI Device are outside the scope of this Technical Specification. It is assumed that some generic onboard platform or network will emerge that can be used for this purpose. In the meantime, the manufacturer of a DSRC device may have to cope with different means for connecting its DRSC device to onboard reader/writer of the ERI-unit.

6.4.3 Lower layers

The ISO 15628/EN 12834 DSRC application layer shall use lower layers as specified in ISO 15628, Clause 9, and Annex E, or in the EU as specified in EN 12834, 6.1.

6.5 Remote access interface

A remote access interface shall be capable of exchanging ERI data protocol units of type SecretKeyEriPdu and encoded conform the PER rules as defined in ISO 8825-2.

An onboard device providing remote access to an ERT shall be capable of transferring ERI protocol data units received from its (cellular network) peer to the ERT and vice versa.

The lower layer (cellular network) protocols (session and lower as applicable) shall comply with international standards.

NOTE If required, an ERI protocol data unit may be segmented and reassembled (in ISO/IEC 7498-1 terminology) as appropriate.

Annex A
(normative)

ASN.1 module definitions

A.1 Overview

This annex contains the following ASN.1 modules:

a) The secret key transaction module;

b) A reduced ISO 15628 module to show how it can be used.

A.2 ASN.1 Modules

NOTE This clause can as a whole be converted to simple text and then be compiled. It contains therefore no additional clause headers and titles.

– SECRET KEY TRANSACTIONS MODULE –

```
EriSecretKeyTransactionsModule
{iso(1) standard(0) iso24535 (24534) secretKeyTransactions (5) version (0)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN

-- Electronic Registration Identification (ERI)
-- Secret Key Transactions

-- EXPORTS everything;

SecretKeyEriPdu ::= CHOICE {
        requestPdu              SecretKeyEriReqPdu,
        reponsePdu              SecretKeyEriRspPdu
        }

SecretKeyEriReqPdu ::= SEQUENCE {
        transactCode            TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
        argument                TRANSACTION.&ArgumentType
                                ({SecretKeyEriTransactions} {@.transactCode}) OPTIONAL
        }

SecretKeyEriRspPdu ::= SEQUENCE {
        transactCode            TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
        result                  TRANSACTION.&ResultType
                                ({SecretKeyEriTransactions} {@.transactCode})
        }

-- TRANSACTIONS

TRANSACTION ::= CLASS {
        &ArgumentType           ,
        &ResultType             ,
        &transactionCode        INTEGER UNIQUE
        }
```

```
WITH SYNTAX {
        ARGUMENT                &ArgumentType
        RESULT                  &ResultType
        CODE                    &transactionCode
        }

SecretKeyEriTransactions TRANSACTION ::= { mutualAuthentication1 | mutualAuthentication2 |
        getSecretKeyEriData | setSecretKeyEriData |
        commisionSecretKeyErt | decommissionSecretKeyErt |
        updateAccessControlList | getCipertextAccessControlListEntry | endOfSession
        }
```

-- Mutual authentication phase transactions

```
mutualAuthentication1 TRANSACTION ::= {
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    1
        }

mutualAuthentication2 TRANSACTION ::= {
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    2
        }
```

-- Data exchange phase transactions

```
getSecretKeyEriData TRANSACTION ::= {
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    3
        }

setSecretKeyEriData TRANSACTION ::= {
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    4
        }

commissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    5
        }

decommissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT                NULL
        RESULT                  NULL
        CODE                    6
        }

updateAccessControlList TRANSACTION::={
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    7
        }

getCipertextAccessControlListEntry TRANSACTION::={
        ARGUMENT                OCTET STRING
        RESULT                  OCTET STRING
        CODE                    8
        }
```

```
-- Session release phase transactions

endOfSession TRANSACTION ::= {
        ARGUMENT                OCTET STRING
        RESULT                  NULL
        CODE                    9
        }

END
```

– Reduced ISO 15628 MODULE –

```
DSRCData { iso(1) standard(0) iso15628(15628) dsrcData (1) reducedVersion (24534) }
DEFINITIONS AUTOMATIC TAGS ::=BEGIN

-- Derived from ISO/DIS 15628 version 2003-05-19
-- The syntax of the module and the ISO 15628 inclusion instructions are corrected to avoid ASN.1 compiler errors.
-- Everything not required to show how ISO 24534 can make use of ISO 15628 is omitted.

IMPORTS
        SecretKeyEriReqPdu, SecretKeyEriRspPdu
        FROM EriSecretKeyTransactionsModule;

Container::=CHOICE{
--      The values 1..16 ommitted
        secrtetKeyEriReqPdu     [19] EriSecretKeyTransactionsModule.SecretKeyEriReqPdu,
                                -- only to be used in an Action-Request
        secrtetKeyEriRspPdu     [20] EriSecretKeyTransactionsModule.SecretKeyEriRspPdu,
                                -- only to be used in an Action-Response
        ... -- extension marker
        }

END
```

Annex B
(informative)

Operational scenarios

B.1 Overview

This annex provides three examples of sessions between an ERT and an ERI reader or writer:

a) An identification session in which the ERI data is read from the ERT;

b) A ERI data read-write session in which ERI data is read from the ERT and new ERI is subsequently written into the ERT;

c) A write and re-commissioning session in which ERI data and security data is written into an ERT.

B.2 Vehicle identification

The communication scenario example for identifying a vehicle is shown in Figure B.1.

This scenario comprises the following steps:

a) The mutual authentication phase with the transactions mutualAuthentication1 and 2;

b) The data exchange phase in which the vehicle is identified with the get secret key ERI data transaction;

c) The session release phase with the end of session transaction.

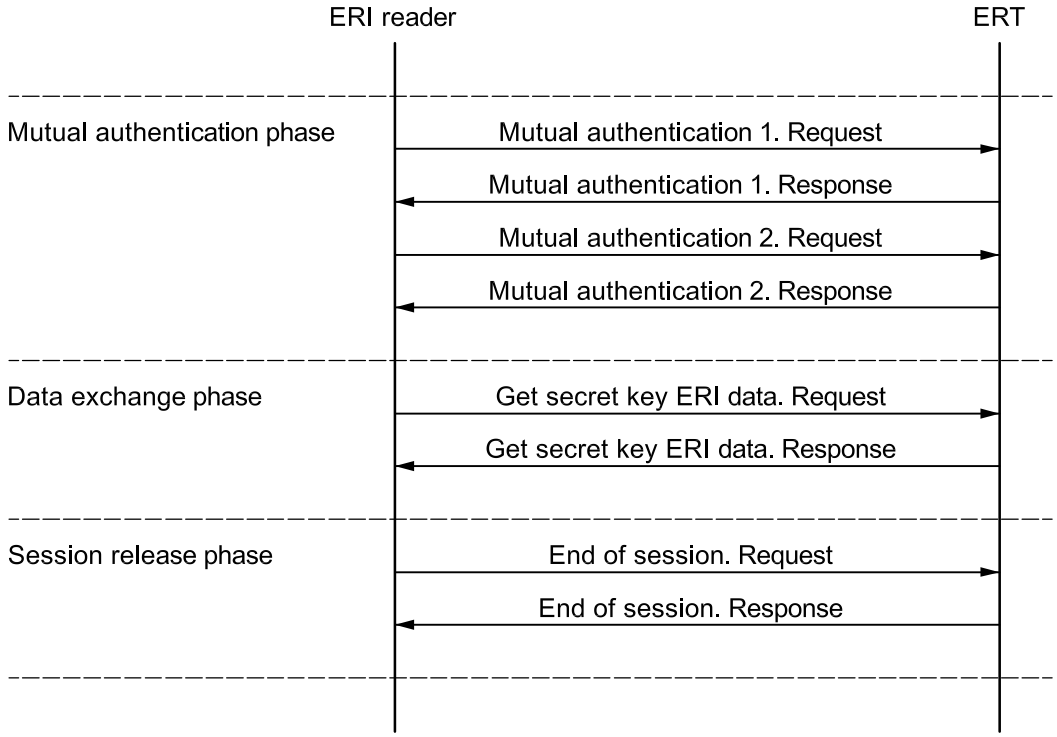


Figure B.1 — Vehicle identification

B.3 An ERI data read-write session

The communication scenario example for reading and writing ERI data is shown in Figure B.2.

This scenario comprises the following steps:

a) The mutual authentication phase with the transactions mutualAuthentication1 and mutualAuthentication2;

b) The data exchange phase in which

   1) the ERI data is read in ciphertext with the get secret key ERI data transaction, and

   2) new ERI data is subsequently written into the ERT with a set secret key ERI data transaction in either ciphertext or in cleartext;

c) The session release phase with the end of session transaction.

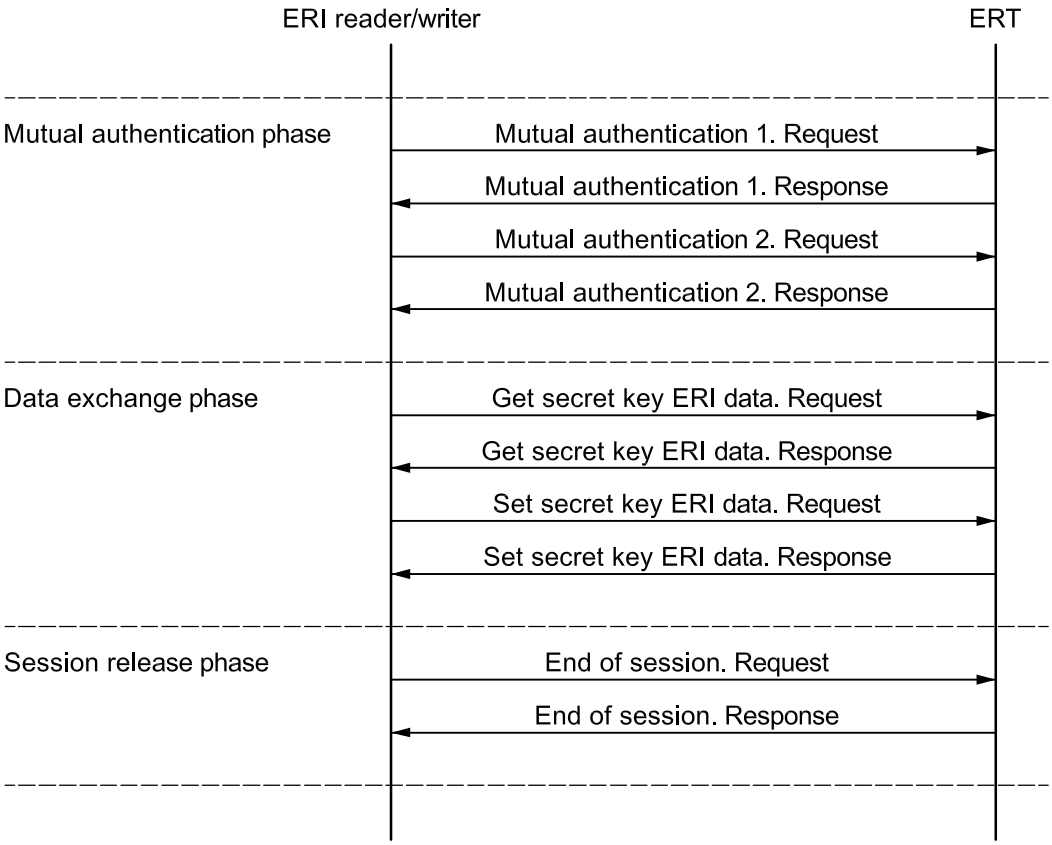


Figure B.2 — ERI data read-write session

B.4 A write and commissioning session

The communication scenario example for writing ERI data and commissioning the ERT is shown in Figure B.3.

This scenario comprises the following steps:

a) The mutual authentication phase with the transactions mutualAuthentication1 and mutualAuthentication2;

b) The data exchange phase in which

   1) new ERI data is written into the ERT with a set secret key ERI data transaction in either ciphertext or in cleartext,

   2) the ERT is commissioned with a commissioning ERT transaction;

c) The session release phase with the end of session transaction.

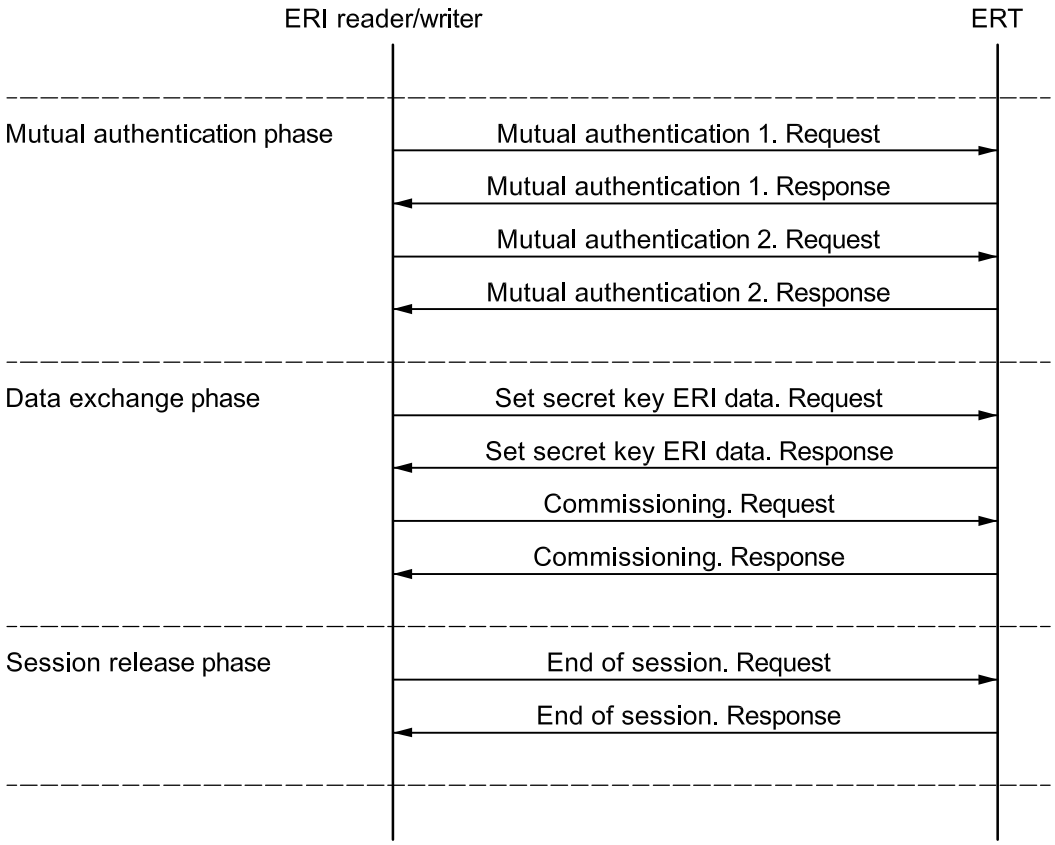


Figure B.3 — Write and commissioning session

Annex C
(normative)

PICS pro forma

C.1 Overview

This annex contains the Protocol Implementation Conformance Statements (PICS) pro forma to be used for ERTs and ERI readers and writers.

C.2 Transactions support

This section applies to both ERTs and ERI readers or writers.

C.2.1 GetSecretKeyEriData

Additional Eri data support	Yes/No
ERT response time for a vehicle identifier in milliseconds	
ERT response time for a maximum length ERI data record in milliseconds	

C.2.2 SetSecretKeyEriData

Supported	Yes/No
Additional Eri data support	Yes/No

C.2.3 CommissionSecretKeyErt

Supported	Yes/No

C.2.4 DecommissionSecretKeyErt

Supported	Yes/No

C.2.5 UpdateAccessControlList

Supported	Yes/No

C.2.6 GetCiphertextAccessControlListEntry

Supported	Yes/No

C.3 ERT Storage capacity

This section only applies to ERTs.

C.3.1 ERI data storage capacity

Description	Max value or range
Max size ERI data record	

C.3.2 Commission data storage capacity

Description	Max value or range
Max length secret key system operator (bits)	
Max value key identifier	
Max number of keys that can be stored with their key identifier	

C.3.3 Authority key storage capacity

Description	Max value or range
Max length secret keys (bits)	
Max value key identifier	
Max number of keys that can be stored with their key identifier	

C.3.4 Generic values

Description	Max value or range
Integers (min and max value)	
Strings (max size)	

Bibliography

[1] ISO/IEC 7498-1, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

[2] ISO 3779, *Road vehicles — Vehicle identification number (VIN) — Content and structure*

[3] ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[4] ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

[5] ISO/IEC 8824 (all parts), *Information Technology —Abstract Syntax Notation One (ASN.1)*

[6] ISO/IEC 9798-1, *Information Technology — Security Techniques — Entity authentication — Part 1: General*

[7] ISO/IEC 9798-2, *Information Technology — Security Techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*

[8] ISO/IEC 10181-1, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

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

[10] ISO/IEC 10646, *Information Technology — Universal Multiple-Octet Coded Character Set (UCS)*

[11] ISO/IEC 11770-2, *Information technology — Security Techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[12] ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*

[13] ISO 14814, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology*

[14] ISO 14815, *Road transport and traffic telematics — Automatic vehicle and equipment identification — System specifications*

[15] ISO 14906, *Road transport and traffic telematics — Electronic fee collection — Application interface definition for dedicated short-range communication*

[16] ISO 15693-3, *Identification cards — Contactless integrated circuit cards — Vicinity cards — Part 3: Anticollision and transmission protocol*

[17] ISO/TS 24534-2, *Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 2: Operational requirements*

[18] ISO/TS 24534-3, *Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 3: Vehicle data*

[19] ISO/TS 24534-4, *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

Price based on 38 pages