

First edition
2011-12-15

AMENDMENT 1
2019-02

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

**Part 5:
Secure communications using
symmetrical techniques**

AMENDMENT 1

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

*Partie 5: Communications sécurisées utilisant des techniques
symétriques*

AMENDEMENT 1



Reference number
ISO 24534-5:2011/Amd.1:2019(E)

© ISO 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

STANDARDSISO.COM : Click to view the full PDF of ISO 24534-5:2011/Amd 1:2019

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

Part 5: Secure communications using symmetrical techniques

AMENDMENT 1

Page 19, 6.2.3.2

Replace definition of SecretKeyEriTransactions by

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

Page 27, 6.3.1

In third paragraph, replace

(CANONICAL-PER) ALIGNED

by

(CANONICAL-PER) UNALIGNED

Page 27, 6.4.1

In first paragraph, replace

(CANONICAL-PER) ALIGNED

by

(CANONICAL-PER) UNALIGNED

Page 31, Annex A

Replace the annex by the following one.

Annex A (normative)

ASN.1 module

A.1 Overview

The following ASN.1 modules are specified in this normative annex:

- The normative module **EriSecretKeyTransactionsModule** {iso(1) standard(0) iso24535 (24534) secretKeyTransactions (5) version1 (1)} in
- The informative module **AviEriDSRCData** {iso(1) standard(0) iso24534 (24534) transactions (2) example1(1) version1 (1)}

In case the ASN.1 specifications given in this Annex are not compliant with illustrations or specifications provided elsewhere in this International standard, the specifications given in this Annex shall prevail.

The ASN.1 modules contained in this Annex will be published on <http://standards.iso.org/iso/24534/-5>.

A.2 Module EriSecretKeyTransactionsModule

```
EriSecretKeyTransactionsModule {iso(1) standard(0) iso24535 (24534)
secretKeyTransactions (5) version1 (1)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN

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 |
commissionSecretKeyErt | 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
}

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

-- Session release phase transactions

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

END

```

A.3 Module AviEriDSRCData

-- Informative example

```

AviEriDSRCData {iso(1) standard(0) iso24534 (24534) transactions (2) example1(1)
version1 (1)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN

IMPORTS

-- From ISO 15628

```

Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList, Attributes, BeaconID, BroadcastPool, BST, Directory, Dsrc-EID, DSRCAApplicationEntityID, Event-Report-Request, Event-Report-Response, EventType, File, FileType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response, ObeConfiguration, Profile, Record, ReturnStatus, Set-Request, Set-Response, Time, T-APDUs, VST FROM DSRData {iso(1) standard(0) dsrc(15628) dsrcData(0) version1 (1)}

-- From ISO 24534-4

SecretKeyEriReqPdu, SecretKeyEriRspPdu FROM EriSecretKeyTransactionsModule

-- From ISO 24534-4

EriRequestPdu, EriResponsePdu FROM ElectronicRegistrationIdentificationTransactionsModule

;

```
ApplicationContextMark ::= CHOICE { -- Container
    integer                [0] INTEGER,
    bitstring              [1] BIT STRING,
    octetstring            [2] OCTET STRING (SIZE (0..127, ...)),
    universalString        [3] UniversalString,
    beaconId               [4] BeaconID,
    t-apdu                 [5] T-APDUs,
    dsrcApplicationEntityId [6] DSRCAApplicationEntityID,
    dsrc-Ase-Id            [7] Dsrc-EID,
    attrIdList             [8] AttributeIdList,
    attrList               [9] AttributeList,
    broadcastPool          [10] BroadcastPool,
    directory              [11] Directory,
    file                   [12] File,
    fileType               [13] FileType,
    record                 [14] Record,
    time                   [15] Time,
    vector [16] SEQUENCE (SIZE (0..255)) OF INTEGER (0..127, ...),
    secretKeyEriReqPdu [19] EriSecretKeyTransactionsModule.SecretKeyEriReqPdu,
                        -- only to be used in an Action-Request
    secretKeyEriRspPdu [20] EriSecretKeyTransactionsModule.SecretKeyEriRspPdu,
                        -- only to be used in an Action-Response
    eriRequestPdu        [70]
ElectronicRegistrationIdentificationTransactionsModule.EriRequestPdu,
                        -- only to be used in an Action-Request
    eriResponsePdu       [71]
ElectronicRegistrationIdentificationTransactionsModule.EriResponsePdu
                        -- only to be used in an Action-Response
}
```

END