# SVENSK STANDARD
# SS-ISO 24534-5:2012

Fastställd/Approved: 2012-01-10
Publicerad/Published: 2012-01-16
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 03.220.20; 35.240.60

**Vägtrafikinformatik – Automatisk fordons- och utrustningsidentifiering – Elektronisk registreringsidentifiering (ERI) av fordon –**
**Del 5: Säker kommunikation med användning av symmetriska tekniker**
**(ISO 24534-5:2011, IDT)**

**Intelligent transport systems – Automatic vehicle and equipment identification – Electronic Registration Identification (ERI) for vehicles –**
**Part 5: Secure communications using symmetrical techniques**
**(ISO 24534-5:2011, IDT)**

# Standarder får världen att fungera

*SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.*

**Delta och påverka**
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

**Ta del av det färdiga arbetet**
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

**Utveckla din kompetens och lyckas bättre i ditt arbete**
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

**Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.**

# Standards make the world go round

*SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.*

**Take part and have influence**
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

**Get to know the finished work**
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

**Increase understanding and improve perception**
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

**If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00**

Den internationella standarden ISO 24534-5:2011 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO 24534-5:2011.

The International Standard ISO 24534-5:2011 has the status of a Swedish Standard. This document contains the official version of ISO 24534-5:2011.



*Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.*

*Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.*

Denna standard är framtagen av kommittén för Vägtrafikinformatik, SIS/TK 255.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

# Contents

Page

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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

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

ISO 24534 consists of the following parts, under the general title *Intelligent transport systems — Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles*:

— *Part 1: Architecture*

— *Part 2: Operational requirements*

— *Part 3: Vehicle data*

— *Part 4: Secure communications using asymmetrical techniques*

— *Part 5: Secure communications using symmetrical techniques*

# Introduction

A quickly emerging need has been identified within administrations to improve the unique identification of vehicles for a variety of services. Situations are already occurring where manufacturers intend to fit lifetime tags to vehicles. Various governments are considering the needs and benefits of electronic registration identification (ERI), such as legal proof of vehicle identity with potential mandatory usages. There is a commercial and economic justification both in respect of tags and infrastructure that a standard enable an interoperable solution.

ERI is a means of uniquely identifying road vehicles. The application of ERI will offer significant benefits over existing techniques for vehicle identification. It will be an enabling technology for the future management and administration of traffic and transport, including applications in free flow, multi-lane, traffic conditions with the capability of supporting mobile transactions. ERI addresses the need of authorities and other users for a trusted electronic identification, including roaming vehicles.

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

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

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

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

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

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

# Part 5:
# Secure communications using symmetrical techniques

## 1 Scope

This International Standard provides the requirements for an electronic registration identification (ERI) using symmetric encryption techniques that are based on an identifier assigned to a vehicle (e.g. for recognition by national authorities), suitable to be used for

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

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

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

— safety related purposes,

— crime reduction,

— commercial services, and

— adhering to privacy and data protection regulations.

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

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

It includes

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

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

— security issues related to the communication with the ERT.

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

## 2 Normative references

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

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

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

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

EN 12834, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

## 3 Terms and definitions

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

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

[ISO 7498-2, definition 3.3.1]

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

[ISO 7498-2, definition 3.3.2]

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

[ISO 7498-2, definition 3.3.4]

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

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

[ISO 24534-3, definition 3.1]

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

[ISO 14814, definition 3.2]

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

[ISO 7498-2, definition 3.3.10]

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

[ISO 9798-1, definition 3.3.5]

NOTE In this part of ISO 24534, the term challenge is also used in case an ERT does not have enabled encryption capabilities and the challenge is merely copied without any secret information applied.

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

[ISO 7498-2, definition 3.3.14]

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

[ISO/IEC 10181-2, definition 3.10]

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

[ISO 7498-2, definition 3.3.15]

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

[ISO 7498-2, definition 3.3.16]

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

[ISO 7498-2, definition 3.3.21]

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

[ISO 7498-2, definition 3.23]