Vägfordon – Utökad säkerhet i datalänkskikt
(ISO 15764:2004, IDT)

Road vehicles – Extended data link security
(ISO 15764:2004, IDT)


Upplysningar om sakinhållet 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.

Postadress: SIS Förlag AB, 118 80 STOCKHOLM
Telefon: 08 - 555 523 10. Telefax: 08 - 555 523 11
E-post: sis.sales@sis.se. Internet: www.sis.se
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>iv</td>
</tr>
<tr>
<td>Introduction</td>
<td>v</td>
</tr>
<tr>
<td>1. Scope</td>
<td>1</td>
</tr>
<tr>
<td>2. Normative references</td>
<td>1</td>
</tr>
<tr>
<td>3. Terms and definitions</td>
<td>2</td>
</tr>
<tr>
<td>4. Symbols and abbreviated terms</td>
<td>5</td>
</tr>
<tr>
<td>4.1 General</td>
<td>5</td>
</tr>
<tr>
<td>4.2 Notation used in the message sequence specified in Clause 6</td>
<td>5</td>
</tr>
<tr>
<td>5. Secured data link configuration</td>
<td>6</td>
</tr>
<tr>
<td>5.1 General</td>
<td>6</td>
</tr>
<tr>
<td>5.2 Architecture</td>
<td>6</td>
</tr>
<tr>
<td>5.3 Protection</td>
<td>7</td>
</tr>
<tr>
<td>5.4 Audit trail</td>
<td>10</td>
</tr>
<tr>
<td>6. Message content</td>
<td>10</td>
</tr>
<tr>
<td>6.1 General</td>
<td>10</td>
</tr>
<tr>
<td>6.2 Message sequence</td>
<td>11</td>
</tr>
<tr>
<td>6.3 Security parameters</td>
<td>16</td>
</tr>
<tr>
<td>6.4 Exception detection and exception response</td>
<td>17</td>
</tr>
<tr>
<td>7. Element description</td>
<td>21</td>
</tr>
<tr>
<td>7.1 General</td>
<td>21</td>
</tr>
<tr>
<td>7.2 Security sub-layer service request parameters</td>
<td>21</td>
</tr>
<tr>
<td>7.3 Security sub-layer service indication parameters</td>
<td>25</td>
</tr>
<tr>
<td>7.4 Security sub-layer service response parameters</td>
<td>25</td>
</tr>
<tr>
<td>7.5 Security sub-layer service confirmation parameters</td>
<td>26</td>
</tr>
<tr>
<td>7.6 Secured Data Transmission Parameters</td>
<td>26</td>
</tr>
<tr>
<td>8. Examples</td>
<td>32</td>
</tr>
<tr>
<td>8.1 Vehicle to remote database</td>
<td>32</td>
</tr>
<tr>
<td>8.2 Tachograph example</td>
<td>35</td>
</tr>
<tr>
<td>8.3 Closed systems</td>
<td>37</td>
</tr>
<tr>
<td>Bibliography</td>
<td>39</td>
</tr>
</tbody>
</table>
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 15764 was prepared by Technical Committee ISO/TC 22, Road vehicles, Subcommittee SC 3, Electrical and electronic equipment.
Introduction

This International Standard is intended initially to supplement ISO 15031-7 in extending the security provisions of, and facilitating access to, remote sources of sensitive data. PC-based external test equipment based on ISO 15031-4, modified to incorporate the facilities described herein, could then access the vehicle using the challenge-response provisions of ISO 15031-7, and the remote source using the extended security offered by the present document.

While this would fully protect the transmission of data from the remote source to the external test equipment, it would leave the data between the external test equipment and the vehicle unprotected, which might be acceptable in a controlled environment. Where the electronic control unit (ECU) is capable of supporting the encryption/decryption burden of full PKI infrastructure, this International Standard offers end-to-end security in an open system in which the participants are not previously known to each other. It also includes provisions for end-to-end security in a closed system where the symmetrical key is established with both participants prior to use and the computing burden is reduced.

It is anticipated that this International Standard will be used, for example, by a vehicle manufacturer to send data to a franchised dealer to enable the programming of an unprogrammed stock ECU or to release immobiliser re-setting codes to approved users. Ultimately, it would protect over-air messages sent directly to a vehicle for software corrections, service interrogation or other remote services.

In the vehicle manufacturer's case, the present document extends the provisions of ISO 15031-7 in respect of data link security to cover the access to data remote from the vehicle, such as that contained in a manufacturer's database — extensions which allow for control and monitoring of such access and thus enhance the security of the data itself. No matter whether the amount of data is small, as in gaining entry to the vehicle, or large, as in a complete code download for powertrain control, it establishes uniform practice for protecting vehicle modules from unauthorized intrusion through a vehicle data link. The security system described represents a recommendation for motor vehicle manufacturers while providing the flexibility for them to tailor their systems to their specific needs.

The vehicle modules addressed are those able to of have solid state memory contents accessed through a data communication link. Improper memory content alteration could potentially damage the electronics or other vehicle components; or risk the vehicle compliance to government legislated requirements or the vehicle manufacturer's security interests. Improper access to secure information could compromise security and privacy of the vehicle or operator.

Other applications are envisaged. In many cases there will be a need for secured data transmission on internal vehicle communication networks such as CAN (controller area network), and between after-market equipment on the one hand, and components of the initial vehicle electronics or other-after market equipment on the other. In particular, this document can be used to enable a tachograph reader to authenticate the data sent by the on-vehicle recorder of the tachograph, for example, in tolling applications. It defines the procedures to establish and use a secured data link and the specific security related data elements. It is communication protocol independent. Another possible implementation is given by the SecuredDataTransmission (84 hex) service defined in ISO 14229-1 on diagnostic services, with whose defined properties its specification of data elements is in line.
Road vehicles — Extended data link security

1 Scope

This International Standard describes an extension of data link protocols for enhancing the security of data transfers between electronic control units (ECUs) connected by a communication network used in road vehicles. It is based on cryptographic methods that include encryption, digital signatures and message authentication codes (MACs). It provides a description of services to establish ECUs as trusted parties in respect of one another and to protect against specific threats. It is applicable to all data links between pairs of ECUs capable of storing and processing secret data so that unauthorized third parties are denied access to it. Parameters are provided to enable the level of security in the data link to be selected.

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 3779:1983, Road Vehicles — Vehicle identification number (VIN) — Content and structure

ISO 3780:1983, Road vehicles — World manufacturer identifier (WMI) code

ISO/IEC 8824-1, Information technology — Abstract Syntax Notation One (ASN.1) — Specification of basic notation — Part 1

ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1

ISO/IEC 9594-8, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8


ISO/IEC 10116, Information technology — Security techniques — Modes of operation for an n-bit block cipher


ISO 11898 (all parts), Road vehicles — Controller area network (CAN)

ISO 14229-1, Road vehicles — Unified diagnostic services (UDS) — Part 1: Specification and requirements ¹)

ISO 14230-4, Road vehicles — Diagnostic systems — Keyword Protocol 2000 — Part 4: Requirements for emission-related systems

¹) Under preparation.
ISO 14816, Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure

ISO 15031-3, Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 3: Diagnostic connector and related electrical circuits, specification and use

ISO 15031-4, Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 4: External test equipment

ISO 15031-7, Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 7: Data link security

ISO 16844-1 (all parts), Road vehicles — Tachograph systems


IETF RFC 2437, PKCS #1: RSA Cryptography Specifications, Version 2.0, October, 1998

IETF RFC 2459, X.509 Internet Public Key Infrastructure Certificate and CRL Profile

SAE J1939 (all parts), Recommended Practice for a Serial Control and Communications Vehicle Network

3 Terms and definitions

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

3.1 certification authority
CA
centre trusted to create and assign public key certificates or, optionally, which may create and assign keys to the entities

[ISO/IEC 11770-1:1996, definition 3.2]

3.2 client
entity initiating the message exchange by sending some request to the other entity

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

[ISO 7498-2:1989, definition 3.3.16]

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

[ISO 7498-2:1989, definition 3.3.21]

---

2) To be published. (Revision of ISO/TS 14816:2000)

3) To be published.
3.5 delay time
DT
time period inserted between access attempts

3.6 data origin authentication
corroboration that the source of data received is as claimed

3.7 digital signature
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to
prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient
[ISO/IEC 9798-1:1997, definition 3.1.3]

3.8 eavesdropping
activity leading to loss of confidentiality, in which a third party obtains data sent between the trusted electronic
units, knowledge of which it is not entitled to possess

3.9 entity authentication
corroboration that an entity is the one claimed

3.10 false access attempt
FAA
error in the received signature, message authentication code or previously unused number

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

3.12 hash-function
function which maps strings of bits to fixed-length strings of bits, such that it is computationally infeasible to
find an input which maps to this output or a second input which maps to the same output

3.13 key
sequence of symbols that controls the operation of a cryptographic transformation
EXAMPLE Encipherment, decipherment, cryptographic check function computation, signature generation or
signature verification
[ISO/IEC 11770-1:1996, definition 3.5]

3.14 manipulation
changing by a third party of data transferred between trusted electronic control units
3.15
masquerade
sending of data by a third party under the pretence that it originates from a trusted electronic control unit

3.16
message authentication code
MAC
string of bits which is the output of a MAC algorithm

[ISO/IEC 9797-1:1999, definition 3.2.5]

3.17
MAC algorithm
algorithm for computing a function which maps strings of bits and a private key to fixed-length strings of bits, such that for any key and any input string the function can be computed efficiently, and that for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i-1 function values

NOTE Adapted from ISO/IEC 9797-1:1999, 3.2.6.

3.18
private key
key of an entity's asymmetric key pair intended to be used only by that entity


3.19
public key
key of an entity's asymmetric key pair which can be made public


3.20
public key certificate
public key information of an entity signed by the certification authority and thereby rendered unforgettable


3.21
replay
resending by a third party of data that was transferred earlier between trusted units, under the pretence that it is “fresh”

NOTE This includes the illicit copying of valuable software destined for one ECU into another ECU.

3.22
repudiation
action by which one of the entities participating in a data transfer afterwards denies having originated the generated data

3.23
secret key
key, established for use by the client and the server, to a message sequence for symmetric encryption and decryption

3.24
server
entity towards which the request of the client is directed

NOTE The server could require information from the client in order to approve the exchange and to react to the request in the intended manner.
3.25
RSA cipher
public key encryption algorithm named after its inventors, Rivest, Shamir and Adleman

4 Symbols and abbreviated terms

4.1 General

AES advanced encryption standard in accordance with ISO/IEC 18033-3
ASN.1 abstract syntax notation one in accordance with ISO/IEC 8824-1
CA certification authority
CAN controller area network
DER distinguished encoding rules in accordance with ISO/IEC 8825-1
ECU electronic control unit
IV initializing value
OID object identifier (ASN.1 type)
SHA-1 secure hash algorithm, Revision 1 (equivalent to dedicated hash-function 3 according to ISO/IEC 10118-3)

4.2 Notation used in the message sequence specified in Clause 6

Cert_\(A\) certificate for the public key of entity \(A\)
Sig_\(A\)[\(X\)] signature of entity \(A\) on data \(X\) (computed using \(A\)'s private signature key), with this notation intended to include a copy of the data \(X\)
[\(X\)]_\(A\) asymmetric encryption of data \(X\) using entity \(A\)'s public encryption key
e_\(K\)(\(X\)) symmetric encryption of data \(X\) using the secret key \(K\)
MAC_\(n\) MAC included in Message \(n\)
n message number
f_\(K\)'(\(X\)) MAC computed on data \(X\) using the key \(K\)
\(K'\) is a variant of \(K\) used for MAC calculation (the same key should not be used for encryption and MAC calculation)
V_\(x\) version number field of the ISO 15764 edition used, where \(x\) is initially 1 and increases with each technical revision of the standard (see 7.6.8)
N_1 previously unused number generated by the client, which should not be confused with the version number (see 5.3.4)
N_2 previously unused number generated by the server
ID_\(A\) unique identifier of entity \(A\), also included in Cert_\(A\) (see 7.6.3)
APar administration parameter indicating the selection of optional parameters and security related options
IV initializing value, a random number used for cipher block chaining in the symmetric encryption procedure
\(\|\) concatenation of two data elements