

INTERNATIONAL STANDARD

ISO 15764

First edition
2004-08-15

Road vehicles — Extended data link security

Véhicules routiers — Sécurité étendue de liaison de données



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.

© ISO 2004

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Symbols and abbreviated terms	5
4.1 General	5
4.2 Notation used in the message sequence specified in Clause 6	5
5 Secured data link configuration	6
5.1 General	6
5.2 Architecture	6
5.3 Protection	7
5.4 Audit trail	10
6 Message content	10
6.1 General	10
6.2 Message sequence	11
6.3 Security parameters	16
6.4 Exception detection and exception response	17
7 Element description	21
7.1 General	21
7.2 Security sub-layer service request parameters	21
7.3 Security sub-layer service indication parameters	25
7.4 Security sub-layer service response parameters	25
7.5 Security sub-layer service confirmation parameters	26
7.6 Secured Data Transmission Parameters	26
8 Examples	32
8.1 Vehicle to remote database	32
8.2 Tachograph example	35
8.3 Closed systems	37
Bibliography	39

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 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 9797-2:2002, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

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

ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

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*²⁾

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*³⁾

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*³⁾

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*¹⁾

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

NOTE Adapted from ISO 7498-2:1989.

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

[ISO/IEC 11770-2:1996, definition 3.1.2]

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

[ISO/IEC 14888-1:1998, definition 4.7]

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

NOTE Adapted from ISO/IEC 9797-2:2002.

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 i th 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

NOTE Adapted from ISO/IEC 11770-1:1996, 3.13.

3.19

public key

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

[ISO/IEC 11770-1:1996, definition 3.14]

3.20

public key certificate

public key information of an entity signed by the certification authority and thereby rendered unforgeable

[ISO/IEC 11770-1:1996, definition 3.15]

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
$\text{Sig}_A[X]$	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

$Data_n$ the data contained in message n

C client

S server

5 Secured data link configuration

5.1 General

The services provided here are independent of the communication protocol between client and server. It is up to individual applications and standards to define how these services are to be encoded at the lower protocol layers. As an example each transaction described between client and server could require multiple transactions at the lower layer protocol.

The standard offers a procedure for securing the data to be transmitted, based on a message sequence with some mandatory elements and some options. A choice can be made among these options according to the security requirements for a given application. The options relate to

- audit trail facilities to assist in the validation of both client and server and to provide the opportunity of a detailed record of the exchange,
- messages to be included to prevent repudiation,
- encryption to prevent loss of confidentiality,
- time-out between sending a request message and receiving the response to it, and
- use of digital signatures to establish a secure connection.

Any examples given are purely to assist understanding and do not suggest that the services must be implemented in these situations.

5.2 Architecture

In its simplest form the system to be covered is shown in Figure 1.



Figure 1 — Overview of system to be protected

It consists of at least one module, the client, communicating with the server through a communication chain. Since, as a minimum, the client must make a request to which the server will respond, two-way point-to-point communication is required. The client may be an entity which requires information held by the server. The server may require further information from the client before permitting the transfer. This simple system can be extended to include further modules at each end. Full end-to-end protection can be provided where encryption/decryption facilities are in place at each end and the intermediate modules are transparent.

In a vehicle module re-programming example, the module in question would be connected to a scan tool which would then be connected via a secure link by land line or mobile telephone to the remote database. Encryption/decryption could be in the scan tool or in the module as required. Details are given in 8.1.

In a tachograph example, the vehicle unit is simply connected to the recording unit by a CAN (controller area network) network. Details are given in 8.2.

In a closed system, where the communicating devices are all under the control of a single entity (e.g. a vehicle manufacturer), certain simplifications to the message exchange are possible. Details are given in 8.3.

For a secured data transmission according to this standard, the data to be transmitted has to be processed in a defined manner by the sender before sending it, and has to be processed again by the receiver before using it. These activities take place within the security sub-layer, according to the layers introduced in the open system interconnection (OSI) reference model. The security sub-layer lies within one of the upper layers specified in the OSI model. It is assumed that the applications on the client and server side decide on the protection type needed, and that the corresponding protection measures, including the management of cryptographic keys within the client and the server, are under the responsibility of the security sub-layer.

5.3 Protection

5.3.1 General

This standard addresses the means of securing the communication path between the client and the server. In doing so it specifies a set of security mechanisms which are designed to provide certain identified security services. These security services have, in turn, been designed to address certain identified threats.

5.3.2 Security threats and services

The security services provided by the scheme specified in this standard address the identified security threats as follows.

- a) **Masquerade** is prevented at the set-up of a message sequence by use of an entity authentication service. Substitution of a malicious third party once the message sequence has been established is prevented by the chaining of the messages using a key established as part of the entity authentication service.
- b) **Replay** is prevented by two different security services:
 - 1) the initial exchange of messages is protected against replay using the entity authentication service;
 - 2) replay of subsequent messages is prevented through the use of a data integrity service.
- c) **Eavesdropping** is addressed by the provision of a confidentiality service.
- d) **Manipulation** is not prevented but is detected by the use of a data integrity service.
- e) **Repudiation** is prevented through the provision of a non-repudiation service.

5.3.3 Use of cryptography

5.3.3.1 General

Before considering the security mechanisms in detail, the following subclauses briefly consider the use of cryptography in the mechanisms specified in this standard.

5.3.3.2 Encryption

Encryption is used to provide confidentiality for transmitted data. Encryption techniques can be divided into symmetric encryption algorithms and asymmetric encryption algorithms. Symmetric algorithms use a shared private key, where the same secret value can be used by both the message sender to encrypt the data and the message recipient to decrypt the data. Asymmetric encryption algorithms require two different values to be used for encrypting and decrypting. These are referred to as public and private keys. The public key and the

algorithm for its use are open to all and can be used to encrypt data, which can only be decrypted using the private key (which is kept secret by its owner).

In this standard the initial exchange is based on the use of public and private keys. Subsequent messages will be encrypted using a symmetric encryption algorithm, whose key is transferred during the initial identification process. This key will be referred to as the secret key. In cases where the two parties already share a secret key, the two messages making up the initial exchange may be omitted.

The public and private keys used to protect the initial exchange will be longer than the secret key and their use will require more computing power. Their use is therefore restricted.

5.3.3.3 Digital signatures

Digital signatures are used to confirm that the signed data has been produced by the entity claimed, and has not been modified since the signature was generated. This is done in such a way that evidence is provided to the verifier which may prevent repudiation of the signed data string by the originator. Signature algorithms use pairs of keys in a similar way to asymmetric encryption algorithms, except that in the case of a signature the private key is used to sign a message, and the public key is used to verify it.

Signatures are used in the scheme specified in this standard to implement the entity and data authentication service, in which an entity proves its identity by providing a signed data string which only it can produce, and which can be verified as genuine and “fresh” by the recipient. Signatures are also used within this standard to create public key certificates, described in 5.3.5.

In summary, signatures are employed by three different types of party within this standard: clients, servers and certification authorities.

5.3.3.4 Message authentication codes

Message Authentication Codes (MACs) are used to guarantee the origin and integrity of messages. MACs are symmetric cryptographic techniques, i.e. they rely on the use of shared secret keys. The sender uses the secret key to compute the MAC, which is appended to the message to be protected. The receiver uses the same secret key with the received message to re-compute the MAC, which is compared with the transmitted value. If the two values agree then the receiver knows that the message has not been tampered with.

Unlike digital signatures, MACs do not provide any protection against the repudiation of messages. This is because both sender and receiver have the same secret key, and hence the receiver could forge a message and its MAC.

5.3.4 Previously unused numbers

The exchange of messages used to provide the entity authentication service makes use of values called *previously unused numbers* and labelled N_1 and N_2 (in fact these values are bit-strings or octet-strings). The client chooses N_1 and sends it to the server, and the server chooses N_2 and sends it to the client. The inclusion of these numbers in responses subsequently received by client and server guarantees that these responses have been newly generated.

It is important that the client chooses N_1 so that it is different from all previous values chosen for N_1 during the lifetime of the current public/private key pair (or, in cases where messages 1 and 2 of the message exchange are omitted and a previously established key K is used, during the lifetime of this pre-established key K). Similar restrictions apply to the server's choice for N_2 (although it is immaterial whether the same value is used for N_1 and for N_2). This can be achieved in many ways. One possibility is for N_1 and N_2 to be chosen at random from all bit-strings or octet-strings of the appropriate length. Another is to use a counter to generate them, although the counter value must be stored securely so that a power failure or other event cannot cause the counter value to be re-initialized. Conveniently, these numbers might be used as job numbers for administrative purposes.