INTERNATIONAL STANDARD

ISO 24101-1

First edition
2008-03-15

Intelligent transport systems — Communications access for land mobiles (CALM) — Application management —

Part 1: General requirements

Systèmes intelligents de transport — Accès des communications pour mobiles terrestres (CALM) — Gestion d'application —

Partie 1: Exigences générales

Reference number
ISO 24101-1:2008(E)

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.

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 24101-1 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

ISO 24101 consists of the following parts, under the general title *Intelligent transport systems — Communications access for land mobiles (CALM) — Application management*:

— *Part 1: General requirements*

— *Part 2: Conformance test*

Introduction

This International Standard is part of a family of International Standards for CALM (Communications access for land mobiles) which determine a common architecture, network protocols and air interface definitions for wireless communications using Cellular 2nd Generation, Cellular 3rd Generation, 5 GHz, Millimeter, and Infrared communications. Other air interfaces may be added at a later date. Air interfaces included in the CALM standards provide facilities for broadcast, point-to-point, vehicle-to-vehicle, and vehicle-to-point communications in the ITS sector.

The purpose of this International Standard is to specify a standardized interface and the functionality necessary for interoperable installation and updating of ITS applications deployed within the CALM architecture in a reliable and secure manner. This International Standard addresses the following requirements:

a) installation of applications on CALM equipment after the equipment has been deployed,

b) updating of applications, including uninstalling, on OBE as well as WAE after the equipment has been deployed, and

c) providing a standardized interface and functionality so that application developers and system operators can successfully perform the functions in a) and b) in a reliable and secure manner.

Intelligent transport systems — Communications access for land mobiles (CALM) — Application management —

Part 1: General requirements

1 Scope

This International Standard specifies structures and methods for application management, including means for installing, uninstalling and updating applications on OBE and WAE deployed in a CALM network in a reliable and secure manner.

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 8824-1:2002, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 9834-1, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree — Part 1*

ISO 21210, *Intelligent transport systems — Communications access for land mobiles (CALM) — Networking Protocols*

3 Terms and definitions

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

3.1
application
software instantiation of an ISO communication model layer 7 (application layer) element, the execution of which in equipment deployed within the CALM/ITS architecture implements services for users

3.2
application management entity
AME
software residing in OBE and/or WAE that manages installation, uninstallation and modification of resident applications

3.3
application management table
AMT
table in an AME that stores management related information for resident applications

3.4
authentication
process by which security credentials, for example a certificate, are verified by an approved process

NOTE The approved process used for verification is not defined in this International Standard.

3.5
certificate
security credential containing information used to verify the identity of the source of the credential, e.g. a manager certificate is sent by the manager of an application to the OBE/WAE and is used by the AME to authenticate the manager. Authentication of the manager is required for further access to the AME

3.6
common file
file containing information that is accessible to (and used by) more than one resident application

3.7
installer
means for installing, uninstalling and modifying applications in OBE or WAE

EXAMPLE Software on a server that is responsible for downloading applications from a (possibly different) remote server over an IP network to OBE or WAE which is connected to the network.

3.8
manager
entity that is responsible for the security management and operation of applications, common files and other entities such as OBE/WAE, installers and operators

3.9
on-board equipment
OBE
equipment installed in a vehicle that exchanges information via one or more radio communication interfaces with other OBE or WAE

3.10
operator
entity that manages and controls an installer at the direction of or the commission by a service provider

3.11
service provider
entity that provides ITS services to users

3.12
test equipment
entity used to verify that installation, uninstallation or modification of an application by an installer in OBE or WAE was performed successfully

NOTE This entity may reside within the installer entity.

3.13
user
entity that uses ITS services provided by a service provider

3.14
wireless access equipment
WAE
equipment installed at fixed locations that exchanges information via one or more radio communication interfaces with OBE and possibly other WAE, and which may have connection to a wide-area network

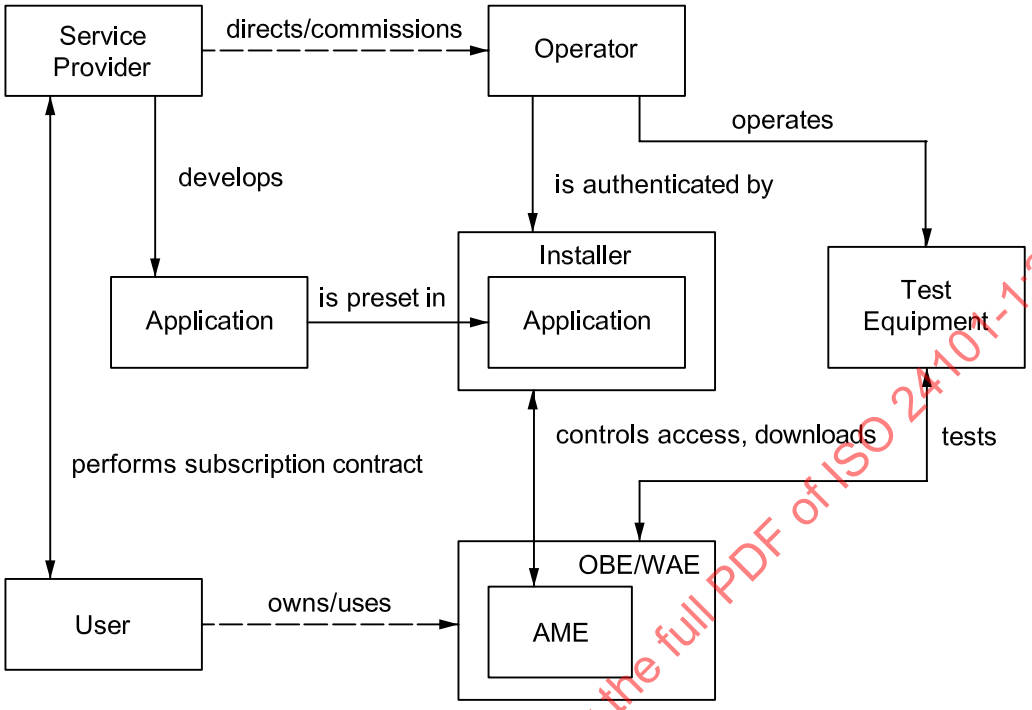
4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AM	Application Management
AME	Application Management Entity
AMT	Application Management Table
API	Application Programming Interface
BER	Bit Error Rate
CALM	Communications Access for Land Mobiles
CME	CALM System Management Entity
CPU	Central Processing Unit
DSRC	Dedicated Short Range Communication
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IP	Internet Protocol
ITS	Intelligent Transport Systems
OBE	On-Board Equipment
OS	Operating System
PER	Packet Error Rate
RSSI	Received Signal Strength Indication
SP	Service Provider
VM	Virtual Machine
WAE	Wireless Access Equipment

5 General structure

The general architecture of the Application Management system is shown in Figure 1.



NOTE 1 In WAE, no user entity exists.

NOTE 2 Service aggregator, who has a role of aggregating application clusters that are provided by different SPs, is not included in this International Standard.

Figure 1 — General architecture of the Application Management system

6 Application installation, uninstallation and modification

The following provide the functionality required for the reliable and secure management of applications in OBE and/or WAE:

a) Application Management Entity (AME) which controls installation, uninstallation and modification of resident applications;

b) Application Management Table (AMT) which contains the management state information for each application;

c) means for communicating between the OBE/WAE and an external installer for the purposes of exchanging information and downloading applications as required.

These elements are shown in Figure 2.

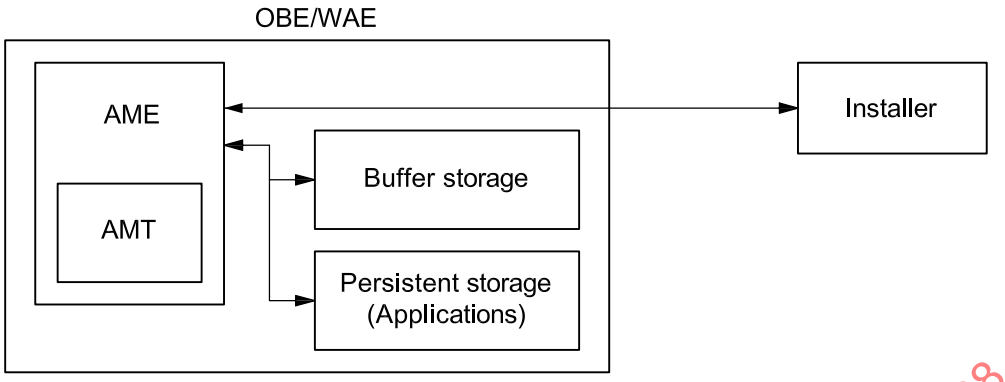


Figure 2 — OBE/WAE resident Application Management elements

6.1 Application Management Entity (AME)

An AME generally consists of the following:

a) an Application Management Table (AMT) in which the status of each resident application is stored (e.g. revision number, date of last modification);

b) means for authentication (e.g. verifying installer certificates) to control access to resident applications;

c) means for transferring the application between the installer and the OBE/WAE;

d) functions for installing, uninstalling and modifying applications;

e) means for ensuring that applications are in an appropriate state before attempting any modification thereto (e.g. ensuring that modification to an application is not attempted while the application is running).

Procedures for installing, uninstalling and modifying applications in an AME are described in 6.4.

6.2 Application Management Table (AMT)

An Application Management Table (AMT) is a table that contains information used in the management of applications. The following information associated with applications is generally useful:

a) application name (file name);

b) date and time of installation or modification;

c) file size;

d) access control information:

   1) keys for verifying manager certificates,

   2) other security related information;

e) additional information:

   1) program version number;

f) other application parameters.

In addition, an AMT may contain useful information that is common to all resident applications, including:

g) available resources (amount of available memory);

h) OBE/WAE manufacturer name;

i) OBE/WAE model and serial number.

6.3 Application loading

6.3.1 Download

A file containing the application is transferred from the installer to the AME and stored (e.g. in buffer memory). This process is called “application loading”.

6.3.2 Download method

Method of downloading an application shall be chosen from the methods in Table 1.

OBE/WAE initiated download means, in this context, a method to submit a request from OBE/WAE to the installer and download an application from the installer (in this process, the installer corresponds to the role of server). Installer initiated download is a method to download from the installer to OBE/WAE.

Table 1 — Download methods

Classification code	Download method
D-1	OBE/WAE initiated download
D-2	Installer initiated download
NOTE OBE/WAE initiated download includes use of network.	

Annex A applies to OBE/WAE initiated download.

Annex B applies to Installer initiated download.

Annex C applies to the classification code D-2 in Table 1, for downloads using DSRC of CALM media.

6.4 Procedures for installing, uninstalling and modifying applications

Procedures for installing, uninstalling and modifying applications are as follows:

a) prior to exchange of application information, the operator and installer authenticate each other and then the OBE/WAE and installer authenticate each other using stored security related information (e.g. public and private keys for creating and decoding digital signatures);

b) after mutual authentications, the installer transfers the application and control information to the AME in the OBE/WAE;

c) the AME uses the control identifier to ascertain whether installation, uninstallation or modification is to be performed;

d) the AME then checks to see if an application with the same application identifier exists in the AMT. If so, and if the control identifier indicates install, an error is returned to the installer;

e) if the control identifier indicates uninstall or modify, the AME checks to see if that application is currently running. If the application is currently running, the AME informs the installer that the application is currently active and the AME enters a wait state until the application completes;

f) when installing an application, the AME checks for sufficient space in memory. If there is sufficient space, the AME installs the application, and then revises the amount of available memory and registers the application in the AMT;

g) when modifying an application, the AME first uninstalls the existing application and revises the amount of available memory, then installs the application [see step f) above];

h) when uninstalling an application, the application is removed, the amount of available memory is revised accordingly, and the uninstall is registered in the AMT.

Annex D presents a flowchart of the procedures for installing, uninstalling and modifying applications.

7 Management structure

7.1 Entity management structure

Entity management structure is described in Table 2. Each object of management shall be managed by the corresponding manager.

Table 2 — Entity management structure

Object of management		Manager	Managing method
Operator		Service provider	On a contract basis
Installer		Operator commissioned by the service provider	Operator authentication, access control
OBE/WAE	Equipment	Owner	On a contract basis
	Application	Service provider	

7.2 Application management structure

Application management structure is described in Table 3. Each object of management shall be managed by the corresponding manager.

Table 3 — Application management structure

Object of management	Manager
Application	Service provider of the application
Common file	Service provider of the common file

7.3 Manager certificate

A manager certificate is a credential containing encoded information used by the recipient to authenticate the source of the credential, e.g. a digital signature generated using a private key, and decoded using a public key allowing entities with access to the public key to verify the sender's identity. Authentication is a prerequisite to allowing access, see 8.3.2.

Managers of applications and common files shall use the appropriate procedures (e.g. encryption and authentication) to ensure their integrity and security.

8 Management of applications and security

8.1 File management

Applications are identified based on their file name. The file name of every application shall be unambiguous.

Naming method and registration authority of the file names shall be in accordance with ISO/IEC 9834-1, and ISO/IEC 8824-1:2002, Annex D, in relation to the object identifier.

8.2 Access to common files

Access to common files shall be made under the authority of manager of the common files.

8.3 Operator authentication and access control

The relationship between operator authentication and access control among the AME, installer and operator entities is shown if Figure 3.

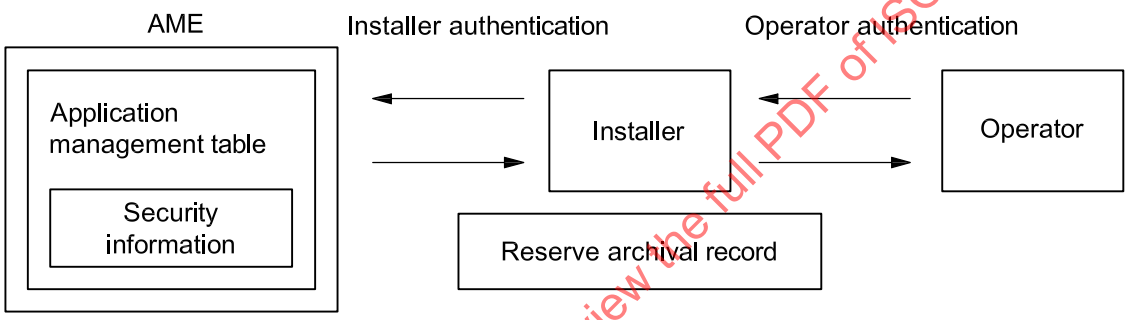


Figure 3 — AME and authentication structure

8.3.1 Operator authentication

Security information (e.g. public key) that allows the installer to authenticate an operator may be stored in the installer in advance.

Mutual authentication of the operator and installer shall precede any exchange of application information.

8.3.2 Access control

Prior to making any changes to resident applications or common files, the AME shall authenticate the source of the requested changes and verify the integrity of the received information, for example, the application to be installed is signed by the application manager and sent to the installer, who, after authenticating the manager, signs and encrypts the message and sends it to the AME who first authenticates both the installer and the application manager before installing the application.

8.3.3 Encryption and authentication

The details of the techniques to be used to ensure data integrity and prevent unauthorized access (e.g. encryption and authentication) are beyond the scope of this International Standard.

9 Installer

An installer shall have the following functions for installer initiated downloads.

9.1 Operator authentication

Prior to sending any command from the operator to the AME, the installer shall authenticate the operator (e.g. by checking the digital certificate sent by the operator along with the commands to be executed.)

9.2 Archival records

The installer shall maintain a record of the operator identification, all operations requested, as well as the results of the operations including time stamps.

9.3 Restoration function

In case the OBE or WAE does not operate normally during tests to be conducted after installing, uninstalling, or modifying an application, the installer shall have a function to restore the equipment to its state just prior to the offending action.

9.4 Function to confirm communication environment

When making downloads wirelessly, the installer shall have a function to enable confirmation of whether sufficient communication quality is attained in the communication environment. The installer shall execute downloads only when this condition is satisfied.

The method of monitoring the communication quality can be one of the methods of detecting RSSI, BER or PER, or a combination of these methods. The details of the monitoring methods and the criteria of the communication quality are not defined in this International Standard.

10 API environment

The API environment shall be one of the classification codes in the following Table 4.

Table 4 — API environments

Classification code	API
APIE-1	API on VM
APIE-2	OS-dependent API
APIE-3	CPU-dependent API

This International Standard recommends APIE-1.

11 Scheduled application updates

Application updates may be scheduled by application managers such that a new or modified application is installed along with a time and date for its activation. Prior to this time and date, the new or modified application shall remain inactive and any applications that are to be modified may remain active. In this case, the current and modified applications are both resident (though only the current one is active).

Scheduled updates shall use one of the methods in Table 5.

Table 5 — Method of the scheduled updates

Classification code	Method
SU-1	OBE/WAE contains a clock. The clock is calibrated by the accurate time and date information included in the communication information from the external equipment. The switching of the application program is executed by comparing the scheduled time and date and the clock information.
SU-2	OBE/WAE contains a clock. The clock is calibrated by the accurate time and date information, which is contained in the radio signal from the Coordinated Universal Time (UTC) station, e.g. GPS, GNSS, or the local standard time station. The switching of the application program is executed by comparing the scheduled time and date and the clock information.
SU-3	OBE/WAE contains a clock. The clock is calibrated by the accurate time and date information via IP network. The switching of the application program is executed by comparing the scheduled time and date and the clock information.
SU-4	OBE/WAE receives the command to switch the program from external equipment at the scheduled time and date. The switching of the application program is executed by the command.

12 Application verification

Testing shall be performed to verify that applications function properly after installation or modification.

The test shall be one of the tests in Table 6.

Table 6 — Tests

Classification code	Test content
T-1	Make wireless communication with the test equipment after installation or modification of an application, to confirm normal operation of the application and no interference given to other applications.
T-2	Do not make wireless communication with the test equipment after installation or modification of an application, but conduct a test-run of the application on a software basis.
T-3	Make a verification check after installation or modification of an application, by reading out the application file.

The details of test procedures are not defined in this International Standard.

13 Transfer to CALM System Management Entity (CME)

AME shall provide the application parameters to CME, which are described in 6.2. For information on the application parameters necessary in CME, see ISO 21210.

Annex A
(informative)

OBE/WAE initiated download

Applying the "OSGi® Service Platform, Specification"[1)] is recommended. The latest edition of the specification applies [3].

NOTE OSGi: The Open Services Gateway Initiative.

1) "OSGi® Service Platform, Specification" is an example of a suitable product available commercially. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by ISO of this product.

Annex B
(normative)

Installer initiated download

B.1 Types of download information

Types of download information shall follow Table B.1.

Table B.1 — Types of download information

Type	Content	Direction
a	Instruction of installation, uninstallation or modification of the application	Installer → AME
b	Result after transaction of installation, uninstallation or modification of the application	Installer ← AME
c	Instruction of reading out the application	Installer → AME
d	Result after transaction of reading out the application	Installer ← AME
e	Instruction of reading out the AMT	Installer → AME
f	Result after transaction of reading out the AMT	Installer ← AME

B.2 Components of download information

The components of download information shall be in accordance with the following, a) to f).

NOTE The installer initiated download method includes not only the communication method but also the non-communication method, such as to use the memory card, etc. Hence, the expression below defines the components of download information.

a) Instruction of installation, uninstallation or modification of the application

```
writeInstruction::= SET {
    sourceCode              [0]  GeneralString,              -- Manager identification code
    destinationCode         [1]  GeneralString,              -- OBE/WAE identification code
    controlIdentifier       [2]  GeneralString,              -- This identifies the difference of
                                                             -- installation, uninstallation or modification
                                                             -- of the application
    aPLIdentifier           [3]  GeneralString,              -- File name of the application
    optionalInformation     [4]  ENUMERATED OPTIONAL,        -- Manufacturer code, program version,
                                                             -- program size, etc. These are not defined
                                                             -- in this International Standard
    securityInformation     [5]  ENUMERATED OPTIONAL,
```

```
applicationData          [6]  EXTERNAL                  -- New program file data in case of
                                                        -- installation or modification. None in case
                                                        -- of uninstallation

-- The "Code", "Identifier" and "Information" are not defined in this International Standard

}
```

b) Result after transaction of installation, uninstallation or modification of the application

```
resultWriteInstruction::= SET {

sourceCode               [0]  GeneralString,            -- OBE/WAE identification code

destinationCode          [1]  GeneralString,            -- Manager identification code

controlIdentifier        [2]  GeneralString,            -- This identifies the result after transaction
                                                        -- of installation, uninstallation or
                                                        -- modification of the application

aPLIdentifier            [3]  GeneralString,            -- File name of the application

optionalInformation      [4]  ENUMERATED OPTIONAL,      -- Manufacturer code, program version,
                                                        -- program size, etc. These are not defined
                                                        -- in this International Standard

securityInformation      [5]  ENUMERATED OPTIONAL,

resultCode               [6]  GeneralString             -- Result code

-- The "Code", "Identifier" and "Information" are not defined in this International Standard

}
```

c) Instruction of reading out the application

```
readInstruction::= SET {

sourceCode               [0]  GeneralString,            -- Manager identification code

destinationCode          [1]  GeneralString,            -- OBE/WAE identification code

controlIdentifier        [2]  GeneralString,            -- This identifies the instruction of reading
                                                        -- out the application

aPLIdentifier            [3]  GeneralString,            -- File name of the application

optionalInformation      [4]  ENUMERATED OPTIONAL,      -- Manufacturer code, program version,
                                                        -- etc. These are not defined in this
                                                        -- International Standard

securityInformation      [5]  ENUMERATED OPTIONAL

-- The "Code", "Identifier" and "Information" are not defined in this International Standard

}
```

d) Result after transaction of reading out the application

```
resultReadInstruction::= SET {
    sourceCode              [0]  GeneralString,              -- OBE/WAE identification code
    destinationCode         [1]  GeneralString,              -- Manager identification code
    controlIdentifier       [2]  GeneralString,              -- This identifies the result after transaction
                                                             -- of reading out the application
    aPLIdentifier           [3]  GeneralString,              -- File name of the application
    optionalInformation     [4]  ENUMERATED OPTIONAL,        -- Manufacturer code, program version,
                                                             -- program size, etc. These are not defined
                                                             -- in this International Standard
    securityInformation     [5]  ENUMERATED OPTIONAL,
    applicationData         [6]  EXTERNAL                    -- Program file data in case of success,
                                                             -- None in case of fail
    -- The "Code", "Identifier" and "Information" are not defined in this International Standard
    }
```

e) Instruction of reading out the AMT

```
readAMTInstruction::= SET {
    sourceCode              [0]  GeneralString,              -- Manager identification code
    destinationCode         [1]  GeneralString,              -- OBE/WAE identification code
    controlIdentifier       [2]  GeneralString,              -- This identifies the instruction of reading
                                                             -- out the AMT
    securityInformation     [3]  ENUMERATED OPTIONAL
    -- The "Code", "Identifier" and "Information" are not defined in this International Standard
    }
```