TECHNICAL REPORT

ISO/IEC TR 29172

First edition
2011-11-15

Information technology — Mobile item identification and management — Reference architecture for Mobile AIDC services

Technologies de l'information — Gestion et identification d'élément mobile — Architecture de référence pour les services AIDC mobile

Reference number
ISO/IEC TR 29172:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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

ISO/IEC 29172 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

Introduction

This Technical Report aims at supporting Mobile AIDC (automatic identification and data capture) services that provide information content to end-users via radio frequency identification (RFID) and optically readable media (ORM) technologies (e.g. ISO/IEC 18004, ISO/IEC 15424, ISO/IEC 29143, ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-6, ISO/IEC 29173, ISO/IEC 29174, ISO/IEC 29175, ISO/IEC 29176, ISO/IEC 29177, ISO/IEC 29178, ISO/IEC 29179, ISO/IEC 29168, and ISO/IEC 9834-9). This Technical Report describes an overall service architecture to provide Mobile AIDC services that are enabled by a set of standards and may be developed by various architectural configurations according to market needs. While each standard in the set focuses only on its specified scope, this Technical Report describes an overall description in relation to relevant standards, and their roles and positions in various implementations.

The overall service architecture deals with all of the relevant standards, their interface relationships and how to incorporate them to develop Mobile AIDC services based on resulting Mobile AIDC technologies.

This Technical Report is presented in terms of the generic reference architecture for Mobile AIDC services and includes the following: descriptions of Mobile AIDC services, reference architecture and service components, service operation procedures, and the relationship among relevant standards to enable the reference architecture.

Information technology — Mobile item identification and management — Reference architecture for Mobile AIDC services

1 Scope

Consisting of Mobile RFID and Mobile ORM services, Mobile AIDC services refer to consumer-oriented information services provided via telecommunication networks and triggered by AIDC technologies such as RFID, linear bar code or two-dimensional (2D) symbol. Although Mobile AIDC services are provided mainly to ordinary consumers, they do not limit other types of end-users such as sales persons and repairpersons. The Mobile RFID services are those triggered by RFID and the Mobile ORM services are those triggered by linear bar code or 2D symbol.

This Technical Report describes a reference architecture for Mobile AIDC services. For example, an RFID tag or a linear bar code or 2D symbol called a “data carrier” is affixed to a movie poster; a Mobile RFID interrogator or a symbol capturing camera, i.e. a Mobile ORM reader, is built into a cell phone; an end-user aims or touches the cell phone to the data carrier on the movie poster; and the corresponding information content is retrieved via the network. This reference architecture does not restrict exploitation of other service architectures and aims at supporting the Mobile AIDC service models described in Clause 5.

This Technical Report includes

- descriptions of Mobile AIDC services,
- reference architecture and service components,
- service operation procedures, and
- relationship among relevant standards to enable the reference architecture.

2 Conformance

This Technical Report does not specify any conformance issue.

3 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 29143, *Information technology — Automatic identification and data capture techniques — Air interface specification for Mobile RFID interrogators*

ISO/IEC 29168-1, *Information technology — Open systems interconnection — Part 1: Object identifier resolution system*

ISO/IEC 29173-1, *Information technology — Mobile item identification and management — Mobile RFID interrogator device protocol for ISO/IEC 18000-6 Type C*[1)]

ISO/IEC 29174 (all parts), *Information technology — UII scheme and encoding format for Mobile AIDC services*[1)]

ISO/IEC 29175, *Information technology — Mobile item identification and management — User data for Mobile AIDC services*[1)]

ISO/IEC 29176, *Information technology — Mobile item identification and management — Consumer privacy-protection protocol for Mobile RFID services*

ISO/IEC 29177, *Information technology — Mobile item identification and management — Object Directory Service for Mobile AIDC services*[1)]

ISO/IEC 29178, *Information technology — Mobile item identification and management — Service broker for Mobile AIDC services*[1)]

ISO/IEC 29179, *Information technology — Mobile item identification and management — Mobile AIDC application programming interface*[1)]

4 Terms, definitions, abbreviated terms and acronyms

4.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29143, ISO/IEC 29168-1, ISO/IEC 29173-1, ISO/IEC 29174, ISO/IEC 29175, ISO/IEC 29176, ISO/IEC 29177, ISO/IEC 29178, ISO/IEC 29179 and the following apply.

4.1.1
access information
formatted data required to locate and retrieve a specified information content

NOTE The access information may be, for example, a URI, formatted according to corresponding format standards.

4.1.2
associated information
data with relation to a Mobile Item Identifier (MII), which may be either access information or information content

4.1.3
content retrieval
process of accessing information content available on a content server

4.1.4
content server
device for storing, handling and providing information content

4.1.5
encoded MII
EMII
data encoded from an MII in conformance with ISO/IEC 29174

1) To be published.

4.1.6
end-user
user who consumes information content offered by a content server

4.1.7
entity
anything (physical or non-physical) having a distinct existence

4.1.8
information content
information resource to be provided in the form of human-enjoyable substance to Mobile AIDC end-users

4.1.9
identifier scheme
ID scheme
numbering system that identifies a specified set of data

4.1.10
Mobile AIDC
automatic identification and data capture (AIDC) technique supporting the Mobile Item Identification and Management (MIIM) technologies of radio frequency identification (RFID) and/or optically readable media (ORM)

4.1.11
Mobile AIDC application
computer program designed to operate in a Mobile AIDC terminal

4.1.12
Mobile AIDC application platform
set of computer instructions as the place to launch a Mobile AIDC application in a Mobile AIDC terminal

4.1.13
Mobile AIDC data processor
MADP
collection of computer instructions designed to convert encoded information into a usable format by using Mobile Item Identification and Management technologies

4.1.14
Mobile AIDC device
electronic equipment, such as a radio frequency identification (RFID) and/or optically readable media (ORM) reader, which is equipped in a Mobile AIDC terminal

4.1.15
Mobile AIDC service
use of a Mobile AIDC application to provide a value to end-users

4.1.16
Mobile AIDC terminal
electronic device equipped with one or more Mobile AIDC devices to support the functions of Mobile Item Identification and Management (MIIM) technologies and applications

4.1.17
Mobile Item Identification and Management
MIIM
AIDC technique that is connected to wired or wireless networks, including sensor specifications, combining radio frequency identification (RFID) with mobile telephony, and combining optically readable media (ORM) with mobile telephony

4.1.18
Mobile Item Identifier
MII
realization of Unique Item Identifier for unique identification of entities to be provided as consumer-oriented information services within mobile telecommunication environments

4.1.19
MII resolution
process of converting a Mobile Item Identifier (MII) into its associated information by means of Object Directory Service (ODS)

4.1.20
Mobile ORM
AIDC technique supporting the Mobile Item Identification and Management (MIIM) technologies of optically readable media (ORM)

4.1.21
Mobile RFID
AIDC technique supporting the Mobile Item Identification and Management (MIIM) technologies of radio frequency identification (RFID)

4.1.22
Object Directory Service
ODS
service to provide a mapping relationship between MII for something physical or virtual and its corresponding associated information

4.1.23
Object Identifier (OID) resolution
process which translates an Object Identifier (OID) into associated information with the OID

NOTE See ISO/IEC 29168.

4.1.24
Object Identifier (OID) Resolution Server
ORS
server-side of OID Resolution System which maintains distributed database of associated information with OIDs

NOTE See ISO/IEC 29168.

4.1.25
user data
information that is optionally additional to identifier, is stored together with the identifier in a data carrier and is intended to be provided to end-users

4.2 Abbreviations and acronyms

2D Two-Dimensional

AIDC Automatic Identification and Data Capture

API Application Programming Interface

B2B Business-to-Business

B2B2C Business-to-Business-to-Consumer

B2C Business-to-Consumer

BREW	Binary Runtime Environment for Wireless
DB	Database
DNS	Domain Name Service
EMII	Encoded Mobile Item Identifier
EPC	Electronic Product Code
ID	Identifier
IP	Internet Protocol
J2ME	Java 2 Platform, Micro Edition
JSR	Java Specification Request
LDAP	Lightweight Directory Access Protocol
MADP	Mobile AIDC data processor
MASP	Mobile AIDC start program
ME	Micro Edition
MII	Mobile Item Identifier
MIIM	Mobile Item Identification and Management
MP3	MPEG-1 Audio Layer 3
MPEG	Moving Picture Experts Group
RA	Registration Authority
REX	Realtime Executive Operating System
RF	Radio Frequency
RFID	Radio Frequency Identification
ODS	Object Directory Service
OID	Object Identifier
ONS	Object Name Service
ORM	Optically Readable Media
ORS	Object identifier Resolution Server
QR	Quick Response
SCM	Supply Chain Management
TCP	Transmission Control Protocol
TID	Tag ID

UII	Unique Item Identifier
URI	Uniform Resource Identifier
URN	Uniform Resource Name
WAP	Wireless Application Protocol
WIPI	Wireless Internet Platform for Interoperability
XOR	eXclusive OR

5 Overview

The Mobile AIDC services have been developed to provide consumer-oriented information to end-users. But the Mobile AIDC services do not limit other information services to business persons such as sales persons and repairpersons because Mobile AIDC technologies do not depend on information and end-user types. They are initially triggered by a linear bar code, a 2D symbol or an RFID tag. They may be classified into reader-based and tag-based types. The reader-based type refers to the case that a Mobile AIDC terminal is equipped with at least one Mobile AIDC device for reading an MII from a data carrier. But the tag-based type refers to the case that a Mobile AIDC terminal includes a data carrier embedding an MII and other Mobile AIDC devices read the MII. The tag-based type includes also the case that a Mobile AIDC terminal displays a linear bar code or 2D symbol on its screen and works as a data carrier by itself.

NOTE The description of Mobile AIDC services does not limit other service types. For example, NFC can provide the Peer-to-Peer communication model between two Mobile RFID devices, which is not covered by this Technical Report. This reference architecture aims at supporting only the service types described at the above paragraph.

Figure 1 shows four examples of reader-based Mobile AIDC applications/services models. This type of Mobile AIDC service is called Business-to-Consumer (B2C) services because a content server in a business domain provides an information service to consumers. Business-to-Business-to-Consumer (B2B2C) services are also possible when information is exchanged between business partners in an enterprise business domain and this B2B information is ultimately delivered to consumers. Mobile AIDC services, however, do not limit enterprise business-oriented use cases and can be provided to not only consumers but also business operators. For example, a repair man or salesman may access business-purposes information through Mobile AIDC technologies.

There are two following characteristics between B2B and B2C AIDC services:

- Mobile AIDC device perspective: B2C Mobile AIDC terminals are equipped with at least one or more Mobile AIDC devices. For instance, a cell phone may be equipped with a camera to capture a linear bar code or 2D symbol and/or also an RFID interrogator to read an RFID tag. Thus controlling Mobile AIDC device(s) and processing MII and relevant data are performed at the same place, for example, cell phone. But B2B AIDC applications work usually with many AIDC terminals distributed within an enterprise domain. Where operation and management of the AIDC terminals are concentrated on an application or middleware host, and controlling AIDC terminals and processing identifiers and relevant user data are not performed at the same place. But every Mobile AIDC terminal is handled by each end-user and Mobile AIDC terminals cannot be managed in such concentrated way. This is the reason why ISO/IEC 15961 is specified as the application interfaces standard between the AIDC terminals and the host and the Mobile AIDC terminals do not need the application interfaces standard.

- End-user perspective: End-users of the B2C model are day-to-day consumers and those of the B2B model are business logics, applications and systems, operators in a work environment, or employees. Thus, the information requirements are different for each group served. Recreational information such as images, audio music, songs, movies, news, games, information, etc. are provided to consumers by the B2C model. But business information content such as the volume of objects, number of boxes, delivery source and destination, expiry date, manufacturer, etc. are provided to business systems and relevant end-users by the B2B model.

By these different characteristics, Mobile AIDC service functions need to be integrated with existing consumer information service infrastructures, and privacy protection toward consumers becomes a critical issue for service providers to penetrate the consumer market with Mobile AIDC services so that the proper security measures will be utilized.

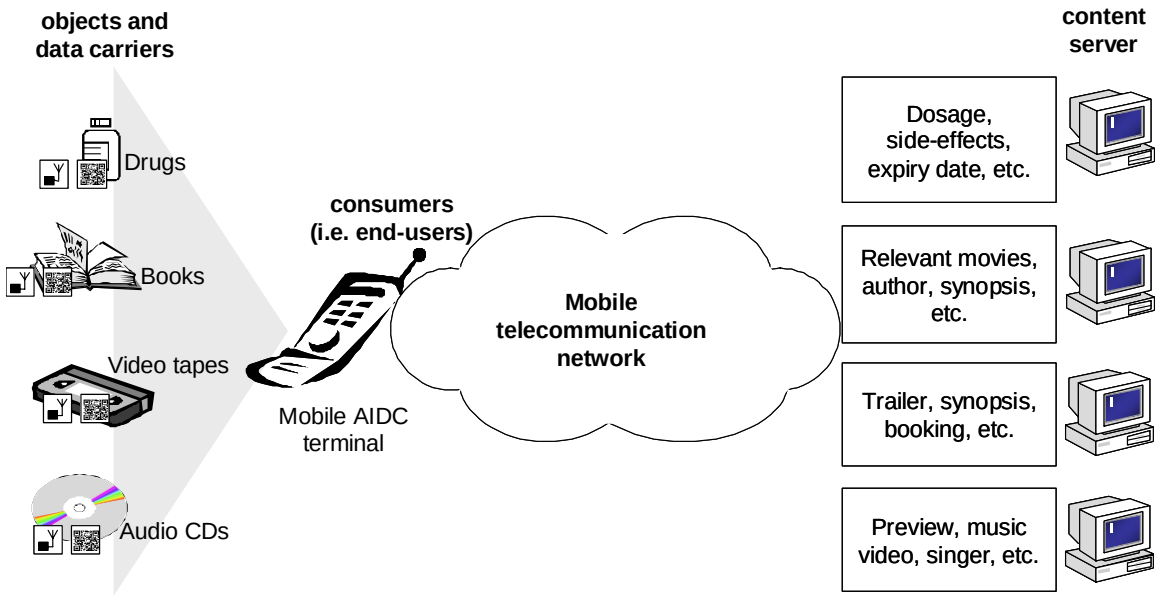

Figure 1 — Use cases of Mobile AIDC applications and services

The methods outlined below allow existing AIDC technologies to communicate with mobile telecommunication networks and their functional entities. The mandatory elements to provide Mobile AIDC services are: MII; Mobile AIDC device such as an RFID interrogator, optical scanner or camera; and a data carrier such as an RFID tag, or a label containing a linear bar code or 2D symbol. The MII is embedded as an EMII in the data carrier; the Mobile AIDC device is equipped in a Mobile AIDC terminal; and the Mobile AIDC device reads or captures the EMII from the data carrier. The Mobile AIDC terminal, consisting of a set of operation functions, then manipulates the MII and finally fetches corresponding information content from a content server. The end-user enjoys the information content provided to its Mobile AIDC terminal.

The scenario described above and illustrated in Figure 1 has been simplified, and there are actually many operational steps and functional entities involved in the process. This Technical Report will identify those steps and describe an overall structure in terms of the reference architecture for which relevant standards are illustrated in Annex A. The Mobile ORM may be developed in a simpler way. Annex B describes a simple implementation case for Mobile ORM services.

6 Generic reference architecture

6.1 General

The generic reference architecture is described below in three ways: communication model among the relevant network entities, including the Mobile AIDC terminal; clarification of their functional service entities; and two core service operations (basic service operation and service broker-assisted service operation).

NOTE In this Technical Report, "*generic*" means that the reference architecture may be applied to most Mobile AIDC service providers and does not limit Mobile AIDC service providers to exploiting their own architectures specifically.

6.2 Communication model

Mobile AIDC services may be developed in various ways. This clause describes only a basic model and a service broker-assisted model. An implementation may utilize a simpler operation model, as described in Annex C, which is not involved with ODS specified in ISO/IEC 29177.

Both basic and service broker-assisted models are optionally implemented because service providers may exploit other communication models and may want to provide only one communication model: one of the two described models or their own model.

6.2.1 Basic communication model

Figure 2 illustrates an RFID tag, a linear bar code or 2D symbol attached to a movie poster. The MII assigned for the movie is contained as an EMII in the data carrier. One or more Mobile AIDC device(s) are built into the Mobile AIDC terminal. A content server maintains the information content associated with the movie. The ODS manages the access information to retrieve the information content identified by the MII where the access information is usually represented as a URI.

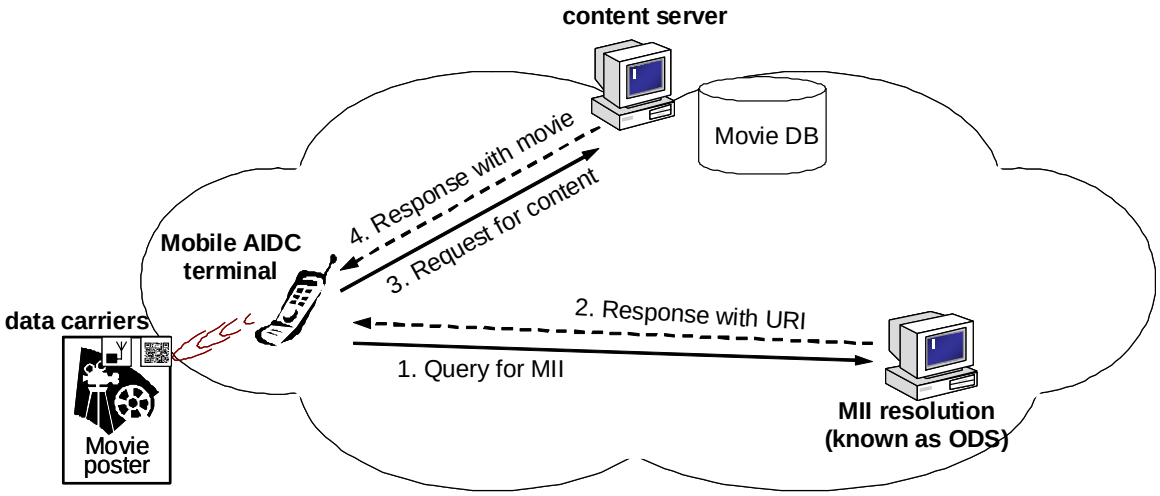

Figure 2 — Basic communication model

Figure 2 assumes the Mobile AIDC terminal has already acquired an MII from one of the data carriers, and illustrates a basic communication model only consisting of two end-to-end operations: MII resolution (steps 1 and 2) and content retrieval (steps 3 and 4). This basic model is not a new one. Every TCP/IP client and server application works in a similar way in the Internet: name resolution and content retrieval. For example, when a Web browser accesses a Web page via a URI, it has to get a network address, i.e. IP, by consulting DNS which resolves a domain name embedded in the URI into the network address. Then the browser retrieves the Web page by connecting to a Web server which is addressed by the network address and contains the Web page. The former operation is the name resolution and the latter one is the content retrieval.

Mobile AIDC, however, has a different resolution target, the MII, instead of the domain name. The MII resolution is the operation that a Mobile AIDC terminal asks the ODS to resolve an MII and receive a corresponding URI. DNS is a typical example of protocol solutions for the MII resolution. There may be other protocol solutions like X.500, LDAP, etc. The content retrieval works through a generic Web access operation.

6.2.2 Service broker-assisted communication model

The basic model may be extended in various ways and those extensions depend on specific implementations. The typical implementation is to incorporate an intermediate broker called the service broker, between the Mobile AIDC terminal and ODS, as shown in Figure 3. The service broker may be simply a proxy for MII resolutions or it may perform additional functions such as filtering MII resolution requests according to end-users. Supporting functions depend on the implementation.

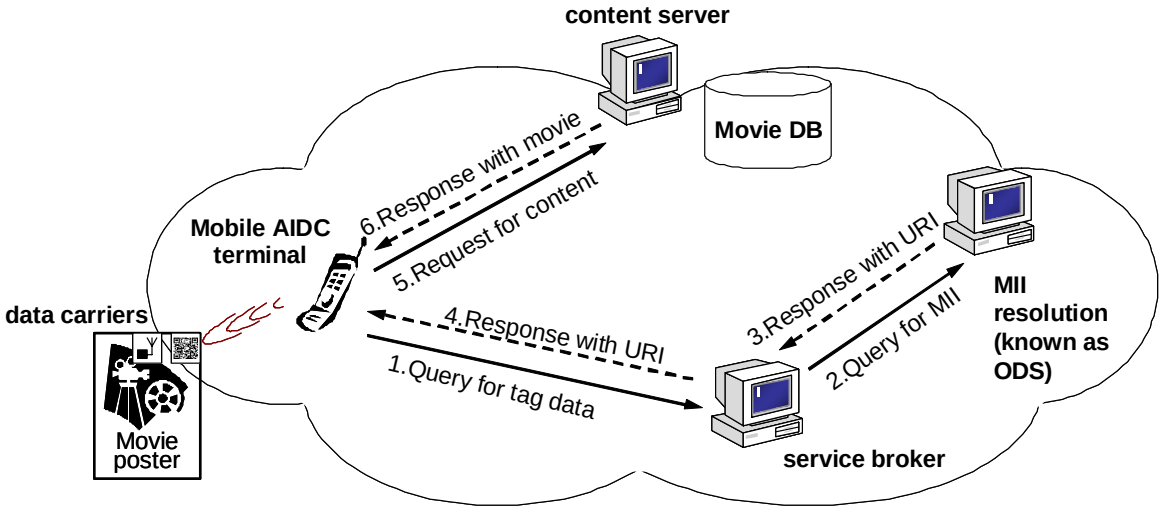

Figure 3 — Service broker-assisted communication model

The benefit of a service broker, as illustrated in Figure 3 above, is to move responsibility for the modification and maintenance of supporting functions and features from the Mobile AIDC terminal to the service broker. This means that a mobile telecommunication service provider doesn't have to manage the Mobile AIDC terminals of its subscribers for any addition, deletion or change. The functions of the service broker are described in ISO/IEC 29178.

6.3 Service entities

Figure 2 and Figure 3 show only the high level functional entities, and each model may consist of sub-entities for specific functions. The high level functional entities, as described below, are classified into data carrier entity, Mobile AIDC terminal entity, MII resolution entity (known as ODS), content server entity and service broker entity.

6.3.1 Data carrier entity

The data carrier entity stores one MII and optional user data. They may be realized in various ways according to the specific AIDC technology, as follows.

6.3.1.1 RF data carrier

The typical example of RF data carriers are RFID tags. An MII is embedded as an EMII in an RFID tag in which radio frequencies conform to ISO/IEC 18000-6 Type C or ISO/IEC 29143.

6.3.1.2 ORM data carrier

The typical examples of ORM data carriers are linear bar codes or 2D symbols. An MII is encoded in the form of a linear bar code or 2D symbol, and printed on a paper or plastic label or other proper media or displayed on the screen of a Mobile AIDC terminal. There are a variety of symbologies available and all of them may be used. ISO/IEC 18004, i.e. QR code, is one example.

6.3.2 Mobile AIDC terminal entity

The Mobile AIDC terminal is a terminal device that end-users utilize to enjoy Mobile AIDC services and includes a set of functional entities which are concentrated on the terminal. Typical entities are illustrated in Figure 4 and Figure 5. The entities illustrated are: the Mobile AIDC device shown as the Mobile RFID interrogator and Mobile ORM reader; the Mobile AIDC application platform; and the Mobile AIDC start

program shown as one of the Mobile AIDC applications. The information browser shown as the WAP browser in Figure 6 is also one of the Mobile AIDC applications. All of them are functional entities of the Mobile AIDC terminal entity.

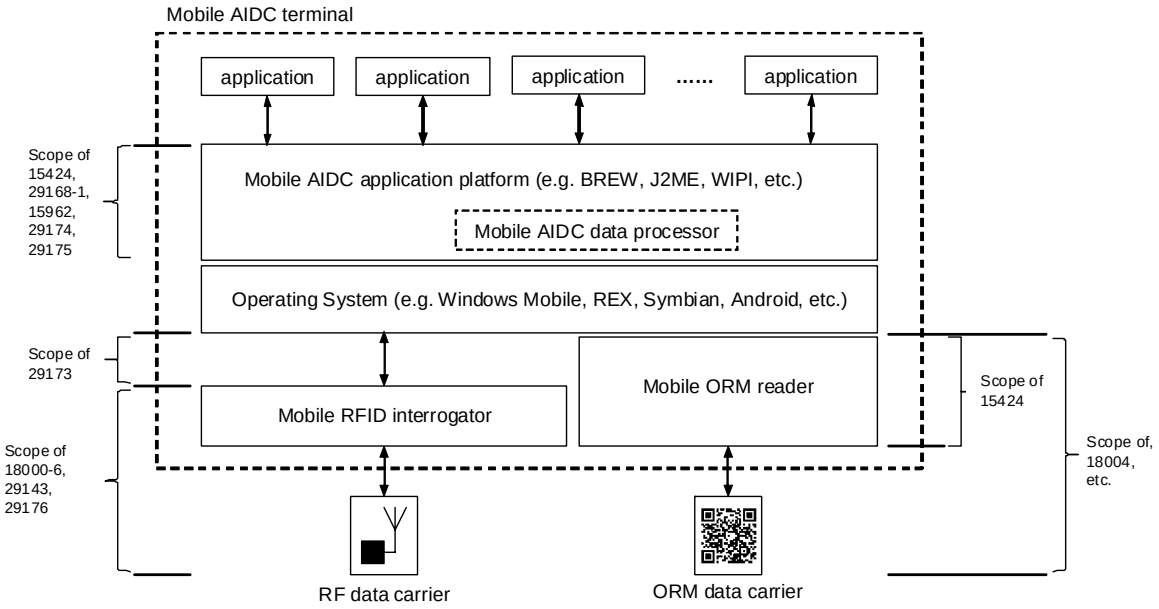

Figure 4 — Mobile AIDC terminal entity configuration: Case 1

The difference between Figure 4 and Figure 5 is the location of the Mobile AIDC data processor (MADP) which carries out the manipulation of the tag data acquired from a data carrier according to Mobile AIDC-relevant standards such as ISO/IEC 15424, ISO/IEC 15962, ISO/IEC 29174 and ISO/IEC 29175. The data processor may be implemented within a Mobile AIDC application platform over which Mobile AIDC applications run; or it may be embedded in a Mobile AIDC application. Thus the function of the API specification of ISO/IEC 29179 for output data from the Mobile AIDC application platform to a Mobile AIDC application depends on the specific implementation. ISO/IEC 29179 supports only Figure 5. A certain API specification for the J2ME application platform in support of Figure 4 was developed as JAVA Community Process JSR-000257 but it is not compliant with ISO/IEC 29179 because it aims at supporting specifically the JAVA platform but ISO/IEC 29179 aims at defining only a high level generic API specification for Mobile AIDC applications and services.

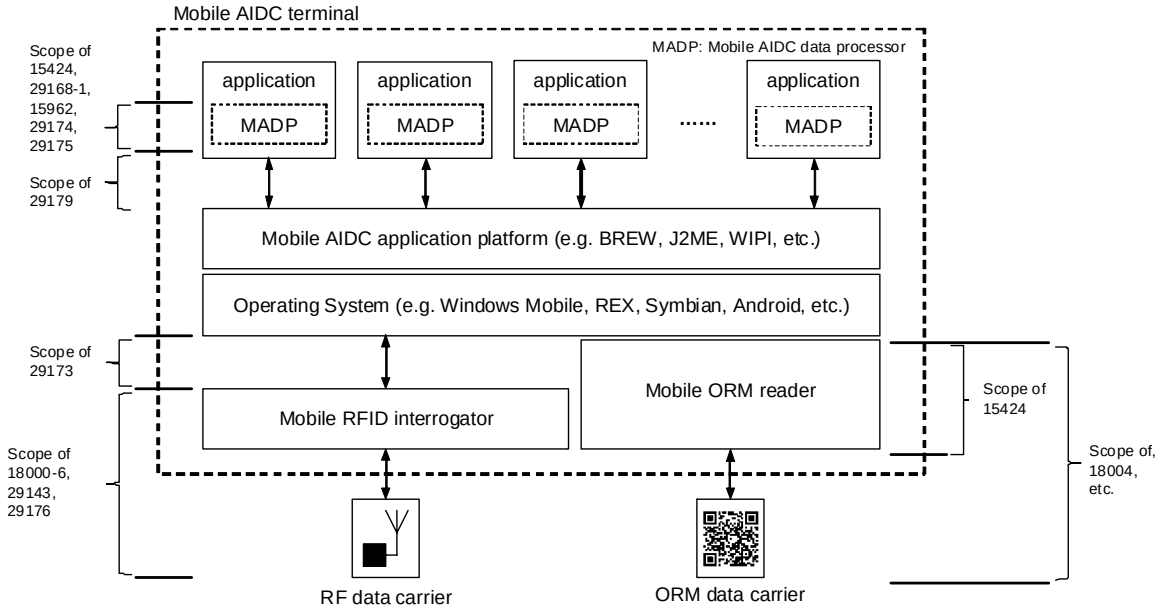

Figure 5 — Mobile AIDC terminal entity configuration: Case 2

6.3.2.1 Mobile AIDC device entity

Figure 4 and Figure 5 show two types of Mobile AIDC devices: a Mobile RFID interrogator and a Mobile ORM reader. The Mobile ORM reader is usually a camera built into a Mobile AIDC terminal.

The Mobile ORM reader consists of a physical camera device to take a picture from a linear bar code or 2D symbol, and a functional program to convert the picture image which results in a tag data where ISO/IEC 15424 and ISO/IEC 18004 are involved. Then the MADP manipulates the tag data.

Since there may be various product vendors of Mobile RFID interrogators, Mobile AIDC terminal manufacturers need a standardized interface between the Mobile AIDC application platform and the Mobile RFID interrogator. ISO/IEC 29173 specifies the interface. The Mobile RFID interrogator communicates with an RFID tag via ISO/IEC 18000-6, ISO/IEC 29143 or ISO/IEC 18000-3 Mode 3. If a privacy protection is required, ISO/IEC 29176 is involved in the Mobile RFID interrogator.

6.3.2.2 Mobile AIDC application platform entity

The Mobile AIDC application platform is not only for Mobile AIDC services and applications but also for conventional applications for Mobile AIDC terminals.

NOTE The Mobile AIDC application platform is an implementation issue. Thus there are various examples such as BREW made by Qualcomm, J2ME made by Sun Mirosystems, and WIPI made by a Korean community.

The conventional application platform provides for downloading and running of application programs for reading newspapers, playing games, sending messages, sharing files, etc. The application programs imply platform-dedicated implementations and run over the application platform that works over a software operating environment.

NOTE There are a few software operating environment examples: Symbian, Qualcomm REX, Apple OS, Google Android, Samsung bada, and Microsoft Windows Mobile.

The existing application platforms may be extended to provide Mobile AIDC applications/services for which ISO/IEC 15424, ISO/IEC 29168, ISO/IEC 15962, ISO/IEC 29174, and ISO/IEC 29175 should be supported in the case of Figure 4. The extended functions are represented as the Mobile AIDC data processor (MADP). ISO/IEC 29179 should be supported in the case of Figure 5.

ISO/IEC 29179 defines a generic and abstract API that may be utilized for API specifications according to the specific platform type. For example, JSR257 is a JAVA-based API specification that defines a Contactless Communication API, i.e. a Java ME optional package containing an application programming interface that allows applications to access certain information on contactless targets, such as RFID tags, smartcards, and linear bar codes or 2D symbols.

6.3.2.3 Mobile AIDC start program entity

The Mobile AIDC start program is a special application in a Mobile AIDC terminal but it is shown as just one of the Mobile AIDC applications running over the Mobile AIDC application platform in Figure 4 and Figure 5.

The start program is the Mobile AIDC application that an end-user of the terminal meets initially when using Mobile AIDC services. When an end-user presses a dedicated button or selects a menu icon, the Mobile AIDC start program is executed. At this time the start program cannot identify what information has to be provided to the end-user.

The start program initially reads an EMII and any optional user data from the data carrier via a set of APIs defined in ISO/IEC 29179. The start program may then invoke functions such as identification and decoding of the EMII, resolution of the OID, and resolution of the MII to understand the MII. Assuming the start program is aware of what is associated with the MII, it invokes a relevant Mobile AIDC application which is usually the information browser. Otherwise a service provider may develop the start program as a one-size-fits-all Mobile AIDC application, which provides not only MII reading but also data presentation functions of the information browser. The choice is an implementation issue according to service/application requirements.

6.3.2.4 Information browser entity

A typical example of the information browser is a mobile web browser such as the WAP browser, Opera Mobile, Microsoft Internet Explorer Mobile, Safari, etc. It provides accessing and browsing the information associated with an MII. Other information browsers such as the MP3 and MPEG players are also possible. The Mobile AIDC start program invokes an information browser associated with the MII and the information browser takes over the control of service operations. Then the information browser provides the information access and browsing to the end-users.

6.3.3 MII resolution entity

Figure 2 and Figure 3 show only an MII resolution entity called Object Directory Service (ODS). The MII resolution, however, may also be involved with Object Identifier (OID) resolution in case that a Mobile AIDC terminal does not include certain information for the MII resolution. Thus the two relevant operations of OID and MII resolutions may be linked. The OID resolution is an optional operation and is always followed by the MII resolution.

6.3.3.1 OID resolution server entity

The OID resolution server is the entity supporting OID resolution. ISO/IEC 15962 defines the use of OID as a higher layer ID to identify ID schemes because there are a variety of ID schemes such as ISO/IEC 15459, ISO 11784, ISO 3297, ITU-T E.164, IETF RFC 791 and 2460, and GS1 numbers such as GTIN, SSCC and GLN, and new ID schemes will be developed in the future according to service requirements. Since two or more different identifiers assigned by different ID schemes may happen to have the same binary data, the higher layer ID called OID is required to identify which ID scheme is applied to the identifiers. ITU-T X.668 | ISO/IEC 9834-9 defines an OID arc, {joint-iso-itu-t(2) tag-based(27)} for dedication to AIDC applications and services, but other OIDs can also be used. A benefit of the dedicated OID arc requiring only two bytes saves memory space.

When a Mobile AIDC terminal reads an EMII from a data carrier, it has to process the EMII according to the format and structure information of the MII. If the terminal has no such information, it cannot manipulate the MII. For example, if a telecommunication device is not aware of the E.164 telephone numbering scheme, it cannot identify which part is country code; which part is national destination code; and which part is subscriber number. Mobile AIDC terminals may include all format and structure information for the specific ID schemes

supported, but they cannot support every ID scheme which exists in the world. If a Mobile AIDC terminal meets an identifier assigned by a new ID scheme identified by an OID, it retrieves the format and structure information of the new ID scheme to process the identifier. The OID resolution server replies with the format and structure information of the specific ID scheme requested by the Mobile AIDC terminal. Then the terminal can recognize and manipulate the identifier. ITU-T X.672 | ISO/IEC 29168-1 defines the OID resolution.

6.3.3.2 Object Directory Service entity

The entities to be provided to end-users as information services of Mobile AIDC shall be distinguished uniquely among themselves. Specific identifiers under a chosen ID scheme are assigned to the entities. The chosen ID scheme is constructed using specific rules of its issuing agency called Registration Authority (RA) to create an unambiguous number for the entities. ISO/IEC 29174 is one of this kind of ID schemes and its qualifier is the OID system defined in ITU-T X.668 | ISO/IEC 9834-9.

Identifiers assigned by ISO/IEC 29174 which specifies Mobile Item Identifier (MII), however, have no meaning by themselves until they are associated with other information, and the association between an MII and its corresponding information shall be resolved. The Object Directory Service (ODS) handles the association and performs the resolution role for the association. ISO/IEC 29177 defines the MII resolution based on the DNS technology.

The ODS does not specify a resolution protocol but utilize an existing resolution protocol, DNS. The ODS specifies only an extension to the resolution message data to incorporate a specific ID scheme where the format of the resolution message data is defined by DNS and the extension handles the supported ID scheme, MII.

An implementation may not be involved with ODS. Annex C describes this use case.

6.3.4 Content server entity

The content server is a network entity that maintains information content for end-users and provides the information content to a Mobile AIDC terminal. The content server may be managed by service providers and/or content providers.

Usually mobile telecommunication operators are represented as service providers because they maintain and provide information content to end-users. The service providers may also be considered as content providers because they maintain information content and handle their content server but content providers may not be service providers and their information content is provided through a service provider by business contracts. The information contents are most often developed and provided through Web technologies. The service providers are also responsible for the whole Mobile AIDC service infrastructure which incorporates MII and OID resolutions, and service broker.

6.3.5 Service broker entity

As shown in Figure 3 and described in Clause 6.2.2, the service broker performs proxy operations for some capabilities of Mobile AIDC terminal entities. Specific functions for proxy operations depend on the relevant standard, ISO/IEC 29178, which also specifies proper interfaces to support them.

6.4 Basic service operation

The basic service operation describes typical service operation steps for the basic communication model. Figure 6 illustrates an actual configuration diagram in a slightly different view for the Mobile AIDC terminal-relevant entities described in Clause 6.3.2. The bearer service means conventional mobile telecommunication services for telephony and data communications.

The Mobile AIDC data processor (MADP) has to be located somewhere as shown in Figure 4 and Figure 5. It may be composed of at least five functions: reader control, user data processing, MII processing, MII resolution and OID resolution as shown in Figure 7. It may include more functions according to relevant standards and implementations. But Figure 7 illustrates only five key functions related to Mobile AIDC

standards. The reader control accesses a Mobile AIDC device; the user data processing handles application-specific user data according to ISO/IEC 29175; the MII processing handles MIIs according to ISO/IEC 29174 and other supporting ID schemes; the MII resolution handles MII resolution for a given MII according to ISO/IEC 29177; and the OID resolution performs OID resolution for a given OID according to ITU-T X.672 | ISO/IEC 29168-1.

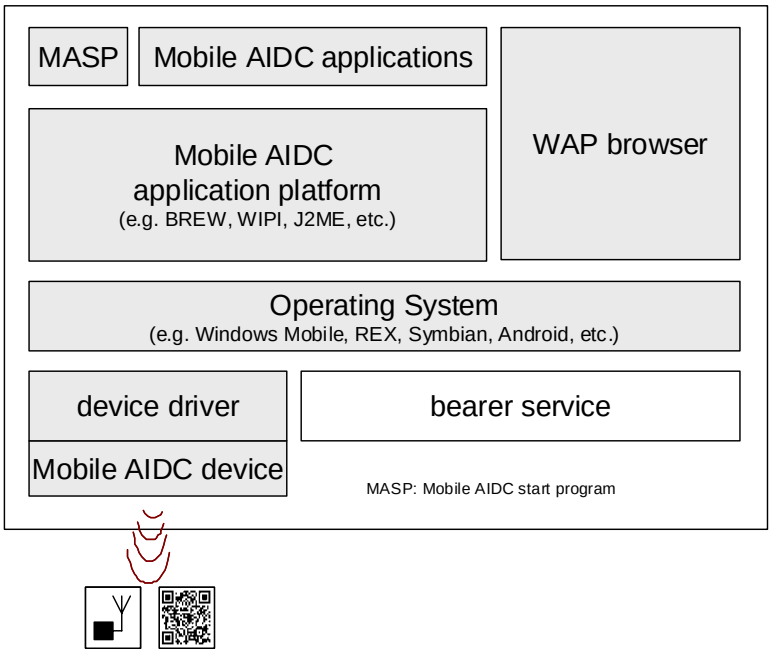

Figure 6 — Actual configuration diagram for Mobile AIDC terminal-relevant entities

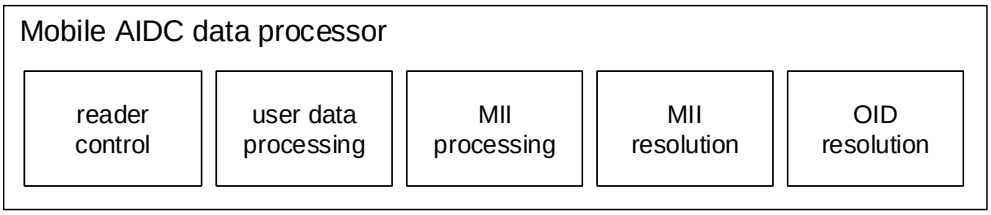

Figure 7 — Functions of Mobile AIDC data processor

In accordance with those service entities and operation functions, procedural reference operations are described below. A typical reference operation procedure is illustrated in Figure 8. The illustration does not show detail operation steps, but only logical operation steps for simplicity. "*Reading tag data*" is involved with the reader control function; "*Identifying MII*" is a part of the MII processing function; "*Requesting OID resolution*" and "*Responding with OID resolution*" is involved with the OID resolution function; "*Decoding MII*" is another part of the MII processing function; *"Decoding user data"* is involved with the user data processing function; "*Requesting MII resolution*" and "*Responding with MII resolution*" is involved with the MII resolution function. Finally "*Requesting HTTP GET*" and "*Responding with HTTP message*" do not belong to the Mobile AIDC data processor and are an ordinary web access operation.

The OID resolution server and ODS in Figure 8 are functionally different but they may be located at the same computer system because they use the same communication protocol, DNS.

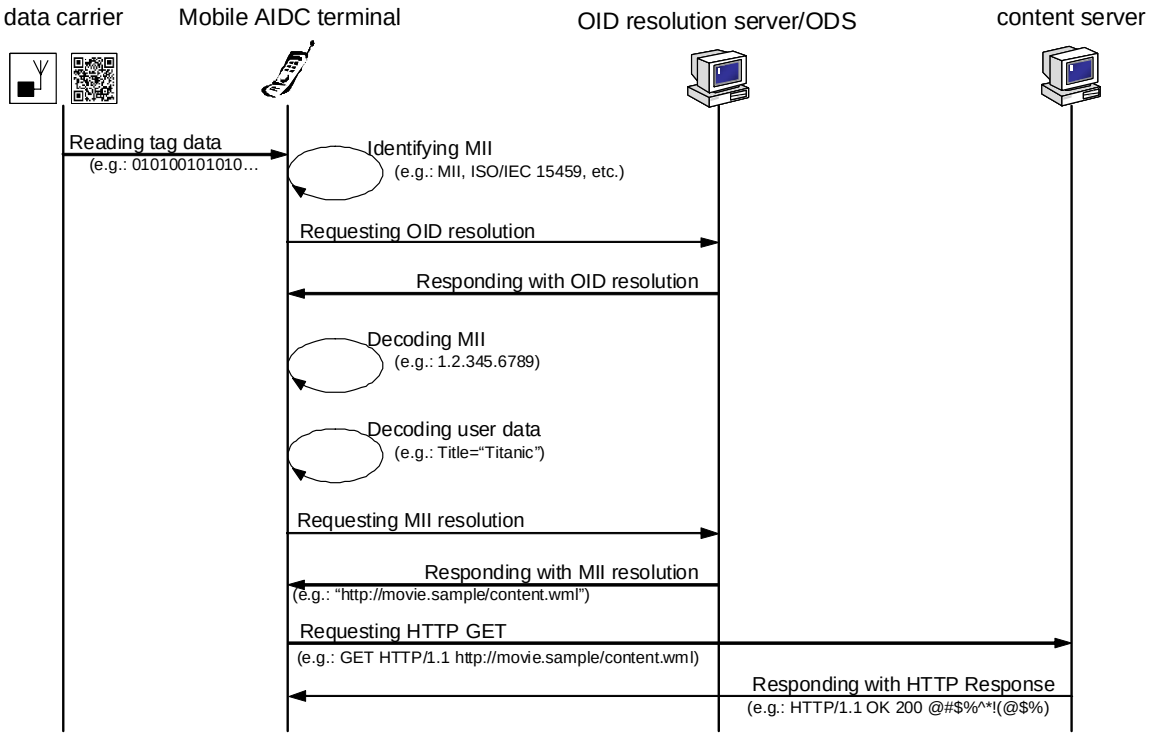

Figure 8 — A reference operation procedure

NOTE The operation step, only "Decoding user data" does not have an operation dependency with other operation steps. Its execution order is an implementation issue.

6.4.1 Data reading

The data reading operation is provided by the reader control function of the Mobile AIDC data processor in Figure 7. As described in Clause 6.2.2.1, a Mobile AIDC device reads tag data from a data carrier. The way to read data depends on the type of a data carrier. If the data carrier is an RFID tag, the Mobile AIDC device will be an RFID interrogator. In a Mobile AIDC service environment, a linear bar code or 2D symbol is usually captured by a camera. Thus data reading techniques are different according to the types of data carriers.

The RFID tag and interrogator have a few alternative solutions for radio frequency bands and relevant air interface protocols. ISO/IEC 18000-6 Type C may be chosen to take advantage of sharing RFID tags between B2B and B2C Mobile AIDC service providers. Moreover integration of B2C with B2B exploits B2B2C information services. But ISO/IEC 18000-6 Type C was developed for industry RFID applications like SCM or inventory management and didn't consider characteristics of Mobile AIDC terminals and mobile telecommunication networks. Therefore Mobile AIDC-oriented air interface is needed and ISO/IEC 29143 is specified to fit the Mobile AIDC service environment. The output of the tag data reading function for RFID tags is the data contained in an RFID tag and encoded in ISO/IEC 15962.

In case of a linear bar code or 2D symbol, a camera captures the symbol without any communication technology. The result of capturing a symbol is just the image that cannot be used by other Mobile AIDC data processor functions, so it needs to be converted into the data that can be handled by the tag data processing function. The data may be encoded initially in ISO/IEC 15962 or symbology-dependent encoding schemes, or might not be encoded if an MII is printed as itself in conformance with the symbology standard. Thus the output of the data reading function for linear bar codes or 2D symbols is the data that is converted from the image data and prefixed with a symbology identifier according to ISO/IEC 15424.

6.4.2 MII identifying

As shown in Figure 8, "*Identifying MII*" is always followed by "*Decoding MII*." The MII processing function deals with these two operations. But the OID resolving operation may intervene between them only if the MII processing function has no relevant information for "*Decoding MII*."

The output of the data reading operation is taken over as input data into the MII processing function to initiate "*Identifying MII*." At first, the MII processing function has to learn what type of ID scheme is used for a given UII by using OID, symbology identifier or some other ways if not using such higher layer IDs. Learning what type of ID scheme is used means not only learning its identity but also getting its format and structure information.

How to learn the identity depends on data carrier technologies. The identity of an ID scheme can be learned from an OID for RFID tags by using ISO/IEC 15962 or from a symbology identifier by using ISO/IEC 15424. If a UII read from a data carrier is learned as an MII by referring to its coupled OID, the MII processing function retrieves the MII format and structure information from a local configuration data or internal database. If the MII processing function finds no relevant information, the OID resolving operation takes over to get the information with the reference to the OID.

NOTE No standard is developed yet for the resolution operation of a symbology identifier.

6.4.3 OID resolving

The OID resolving operation retrieves the format and structure information for a specific ID scheme identified by an OID. The input of an OID resolution is an OID and the output is a format and structure information for the ID scheme provided by an OID resolution server as described in Clause 6.3.3.1.

The OID resolution may not be a simple *"request and response"* operation and it depends on the standard ITU-T Rec. X.672 | ISO/IEC 29168-1 which defines specific protocol procedures with protocol message formats.

6.4.4 MII decoding

Assuming the format and structure information for a given MII is known, the MII processing function decodes raw binary data of the MII into sub-MII elements which may be presented in various ways. For example, if the MII is learned as an E.164 number, the MII processing function converts the raw data of the MII with the E.164 format and structure information into something like "*1.2.345.6789*" if using the dot notation for the delimiter of sub-MII elements.

How to present sub-MII elements is an implementation issue for the MII processing function and the dot notation is one example. URN is another example.

6.4.5 User data decoding

The user data decoding operation converts raw data of the user data contained in a data carrier and encoded in ISO/IEC 29175 into user data elements such as title, name, expiry date, price, manufacturer name, etc. This operation does not depend on other operations except for the data reading operation, which means that it may be executed at anytime after the data reading operation.

Following is one of use cases for the user data: a Mobile AIDC device may read multiple MIIs concurrently at a time while reading dense data carriers. An end-user cannot select one because MIIs are not distinguishable by themselves. If titles or names, however, display on a Mobile AIDC terminal screen, an end-user can select one easily. In this case, the user data decoding operation needs to be executed before the MII identifying operation.

In other cases, titles or names may be retrieved through information retrieval operations from the networks. But this takes some time, over 10 seconds in the worst case due to opening data network and retrieving user data.

6.4.6 MII resolving

Usually ID schemes appear in the form of a series of numbers or alphanumeric characters. An MII assigned by such ID schemes does not have application-specific meaning until it is associated with certain information for a target object to which the MII is allocated. This association is resolved by the MII resolution. An MII may have multiple associations.

ISO/IEC 29177 specifies the MII resolution operation for Mobile AIDC services as described in Clause 6.3.3.2. The input data for an MII resolution is an MII and the output data is an associated information (e.g. information content like audio, video, text or image, or access information like a URI). But the resolution result depends on MII resolution protocols. For example, X.500 can support both types of information content and access information but DNS can support only the type of access information. ISO/IEC 29177 utilizes DNS for the MII resolution protocol to take advantage of the widely-deployed existing DNS infrastructure.

The output data of MII resolutions is usually URIs because the information contents are most often provided by web technologies and retrieved through URIs by information browsers.

6.4.7 Information retrieving

The information retrieving operation is initiated by the information browser described in Clause 6.3.2.4. Typical examples of the information browser are mobile web browsers supporting conventional web information access. The output data (e.g. URI) of an MII resolution replaces the input data to the information browser and an end-user is able to retrieve the corresponding information content.

6.5 Service broker-assisted service operation

Figure 3 shows the communication model to be incorporated with the service broker described in Clause 6.3.5. ISO/IEC 29178 defines supported proxy functions of the service broker with application interfaces for Mobile AIDC terminals. It specifies only two proxy functions: MII recognition and MII resolution. The former one is the same with what the MII identifying and MII decoding operations specify. The OID resolution also is involved optionally as explained before. The standard defines Web-based application interfaces for the service request and response. Figure 9 shows a reference operation procedure.

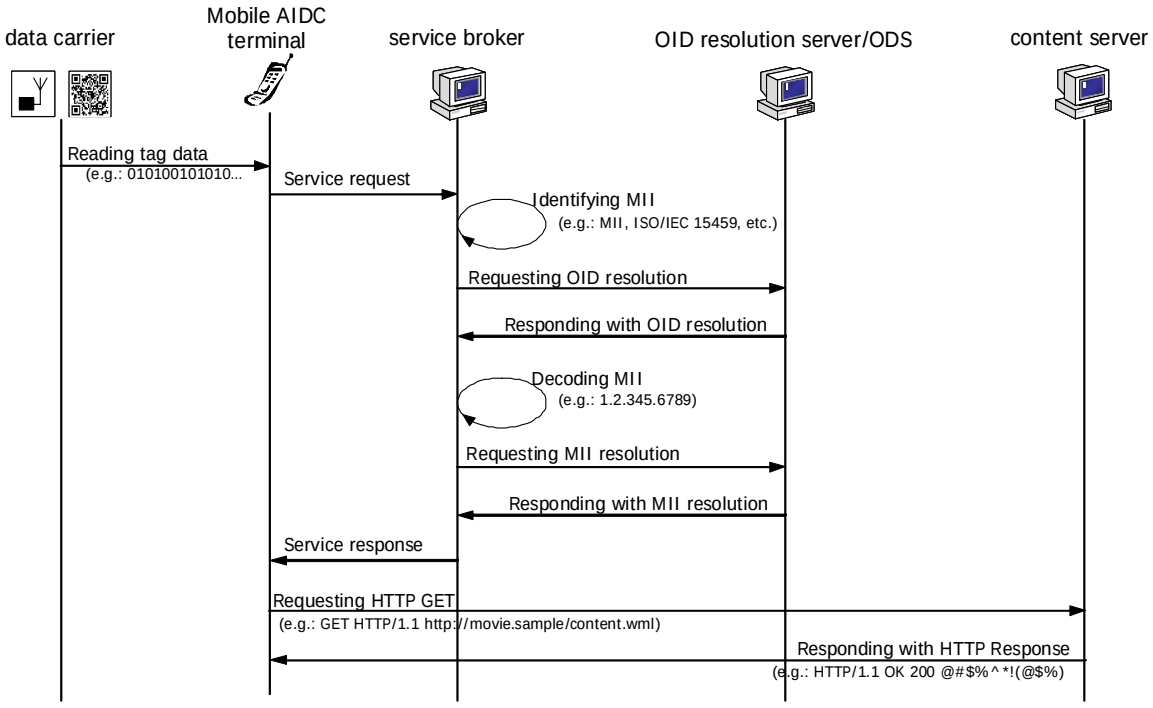

Figure 9 — Service broker-assisted reference operation procedure

6.6 Privacy-protected service operation

Mobile RFID may be a cause of privacy concerns because unauthorized readers might be able to read an MII, TID and User memory banks of ISO/IEC 18000-6C tags and ISO/IEC 18000-3m3 tags. Unauthorized readers could gather specific information about the object assigned with an MII if they are able to analyze the MII coding rule. Thus Mobile RFID services need to support a privacy protection feature to end-users.

ISO/IEC 29176 defines a privacy protection protocol between an RFID tag and a Mobile RFID interrogator. The goal of the privacy protection protocol is to conceal the MII. There three following assumptions to support the privacy protection protocol:

- It is assumed that RFID tags for the privacy protection protocol supports the "*Access*" command of ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 Mode 3; and
- It is assumed that RFID tags for the privacy protection protocol supports the non-zero-valued access password.
- Privacy protection protocol does not preclude other methods of securing an RFID tag.

The protocol consists of five phases as follows:

1) Transiting to the "*secured*" state for an RFID tag: when an end-user buys an item with an RFID tag, the end-user changes the state of the data carrier to the "*secured*" state;

2) Acquiring the original access password for the data carrier: if the data carrier has no access password, i.e. all zero-valued access password in the data carrier, this step is skipped. Otherwise the end-user shall get the access password properly and how to get it is out of scope;

3) Generating end-user's new access password and cover-coding the MII: assuming the access password is known, the end-user generates a new access password and the MII is cover-coded. The default cover-coding algorithm is the bit-wise XOR (eXclusive OR);

4) Updating memory banks: the end-user overwrites the old access password and the MII with the new access password and the cover-coded MII;

5) Locking memory banks of the data carrier: the end-user locks the data carrier to protect it from writing of unauthorized end-users.

Then only the valid end-user can read and understand the data of the protected RFID tag.

Annex A
(informative)

Interface relationship for Mobile AIDC standards

A.1 Introduction

This Annex describes Mobile AIDC-relevant standards and shows an interface relationship which illustrates where each standard is positioned and applied for communication between two parties.

A.2 Relevant Mobile AIDC standards

Clause 3 lists normative references of Mobile AIDC standards.

A.3 Interface relationship for Mobile AIDC standards

Figure A.1 illustrates an overall diagram of Mobile AIDC standards from an interface relationship point of view. Some, such as ISO/IEC 15962 and ISO/IEC 18000-6 Type C, are not shown because they have already been perceived as basic standards. Figure 4 and Figure 5 also show a complementary view.

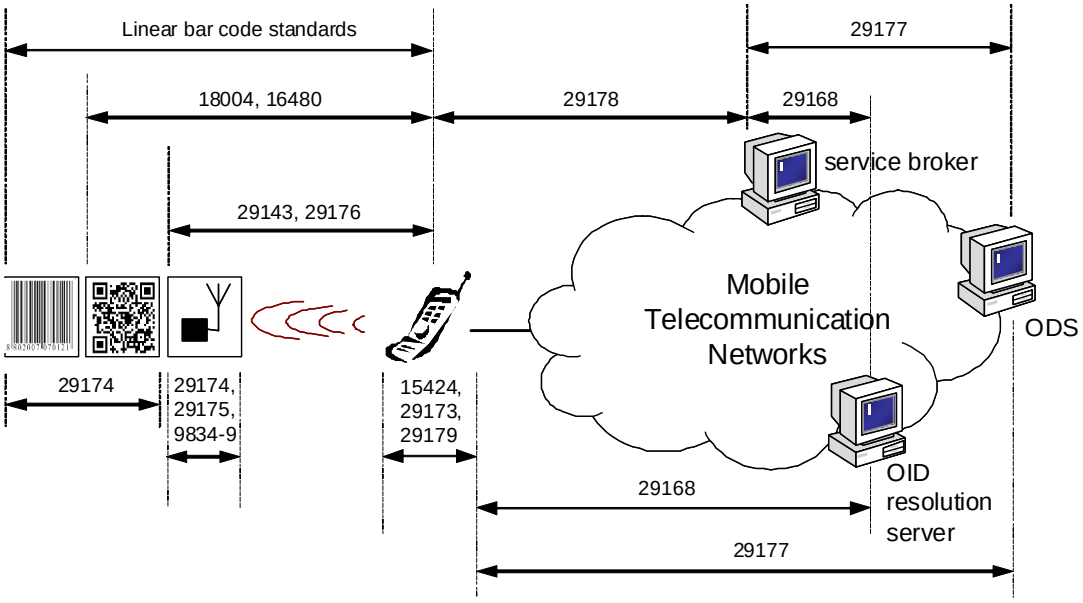

Figure A.1 — Standards relationship diagram

Figure A.1 shows only three types of data carriers: linear bar code, 2D symbol and RFID tag. But other types of data carriers may be possible. Various linear bar codes and 2D symbologies may be used for Mobile ORM services and the choice is an implementation issue for Mobile AIDC service providers. ISO/IEC 18004 is a typical 2D symbology example and is illustrated between the 2D symbology label and the Mobile ORM terminal where the 2D symbol is captured and delivered to the Mobile ORM terminal. Mobile RFID may adopt ISO/IEC 18000-6 Type C and ISO/IEC 29143 to take advantage of existing wide deployment and better applicability for Mobile RFID services. Mobile RFID services may cause privacy concerns to end-users. ISO/IEC 29176 defines how to incorporate ISO/IEC 18000-6 Type C to support privacy protection.

Data carriers include one MII and optional user data for which the basic encoding format is ISO/IEC 15962 for RFID tags. ISO/IEC 29174 defines an ID scheme named as "*Mobile Item Identifier*" to support Mobile AIDC applications and services. The MII is written in or on data carriers. ISO/IEC 29175 specifies types of user data and corresponding encoding formats that do not specify any encoding format extension but defines how to encode each user data type with conforming to ISO/IEC 15962. This basic encoding format standard specifies the usage of OID to identify what kind of ID scheme is used for a given MII. Various OID arcs may be used for this purpose. But ITU-T X.668 | ISO/IEC 9834-9 defines {joint-iso-itu-t(2) tag-based(27)} for dedication to Mobile AIDC services.

There are three standards wholly applied to a Mobile AIDC terminal. When a Mobile RFID interrogator is installed in a Mobile AIDC terminal, it is required to communicate with the existing hardware platform. ISO/IEC 29173 specifies a device control protocol between them. ISO/IEC 29179 defines application programming interfaces to provide Mobile AIDC service functionalities to Mobile AIDC applications. ISO/IEC 15424 is used to specify a symbology identifier for a certain linear bar code or 2D symbology. But the symbology identifier is not encoded into the linear bar code or 2D symbol.

ISO/IEC 29168 defines the generic OID resolution protocol and ISO/IEC 29177 specifies the MII resolution protocol based on DNS. It does not define any protocol extension but does define some message syntax extensions to support the MII resolution.

ISO/IEC 29178 defines the service broker and specifies interfaces between a Mobile AIDC terminal and the service broker.

Annex B
(informative)

An implementation case of Mobile ORM

B.1 Introduction

The Mobile ORM service platform may be implemented differently from the generic reference architecture specified for Mobile RFID and Mobile ORM service providers. The only difference is the data carrier type with different data capturing techniques. This architecture may be more simplified for Mobile ORM services and a different implementation from the generic reference architecture may be exploited.

B.2 Description of Mobile ORM implementation case

An RFID tag contains encoded data for an MII and optional user data according to ISO/IEC 15962. But a printed linear bar code or 2D symbol may embed an MII that is encoded in a linear bar code or 2D symbology without further encoding by a standard such as ISO/IEC 15962, and may be decoded into only the MII. ORM, especially 2D symbol, can store the URI directly according to ISO/IEC 15434. In these cases, consumers can visit a content server directly after they read the 2D symbol. Thus, some of the functional entities of the generic reference architecture cannot be used for Mobile ORM services and a proprietary implementation may be possible.

Annex C
(informative)

An implementation case of non-ODS

C.1 Introduction

Usually an MII is composed of digits or alphanumeric digits and is meaningless until it is associated with information content. The association between MII and information content is handled by ODS.

When a Mobile AIDC terminal sends an MII to the ODS, it receives the associated information from the ODS. This response operation may be performed in two ways: 1) the ODS can handle information content and responds with them directly; 2) or it can handle only the access information for information content and a content server handles the information content. The former case takes just one network operation to get the information content, but the latter case takes two network operations: one for acquiring the access information and the other one for retrieving the information content. The ODS defined in ISO/IEC 29177 supports only the latter case: only the access information for the target information content.

The Mobile AIDC service environment operates based on the latter case for easy management of relevant entities. Thus ODS is always involved. But a specific implementation does not have to be involved with ODS.

C.2 Description of non-ODS implementation case

Usually the access information for information content is represented as a URI. A Web browser retrieves the information content via a URI as an input data. The key issue is how to get the URI that is usually acquired from the networks via the ODS. It, however, may be acquired from a data carrier.

A data carrier may embed a URI in the user data area or MII area. When a Mobile AIDC terminal reads such a URI from a data carrier, it does not need an MII resolution and can retrieve the information content directly via the URI. As a similar example, a Mobile AIDC terminal may read an E.164 telephone number contained in a data carrier and make a call for the number directly without an MII resolution from an MII to the number.

Annex D
(informative)

A reference operation procedure for Mobile AIDC terminal-relevant entities

D.1 Introduction

Clause 6.3.2 describes Mobile AIDC terminal-relevant entities for which this Annex explains a reference operation procedure of theirs.

D.2 Reference operation procedure

The only program that an end-user meets initially to use Mobile AIDC services is the Mobile AIDC start program that may be invoked by a dedicated button or a menu icon. The start program depends on data carrier technologies. Linear bar codes and 2D symbols can be captured by a camera and RFID tags can be interrogated by an RFID interrogator. Thus two start programs are required to control the camera and the RFID interrogator.

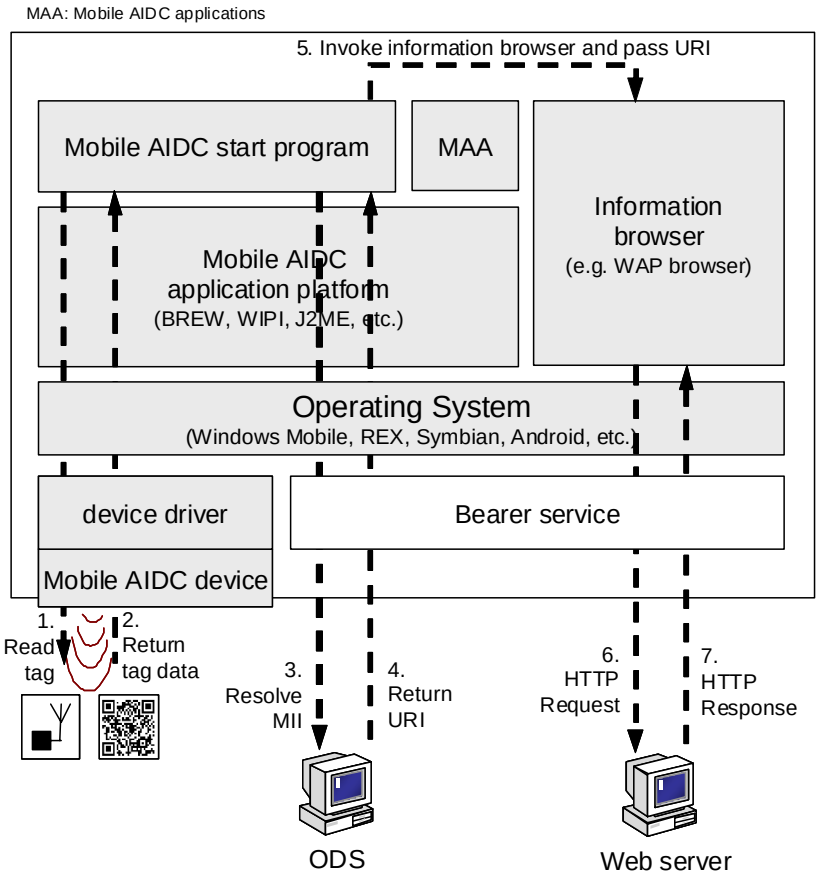

Figure D.1 — Reference operation procedure for Mobile AIDC terminal entities

The Mobile AIDC start program initiates the first operation step: reading a data carrier; and getting data from the data carrier (see Clause 6.4.1 in detail). An MII is returned from the data after proper data processing (see Clause 6.4.2, 6.4.3 and 6.4.4 in detail). The start program then triggers an MII resolution process to resolve the MII into a corresponding URI. Finally it invokes the information browser with passing the URI into the input argument and retrieves an information content associated with the MII through a Web message exchange.

Bibliography

[1] ISO 3297:2007, *Information and documentation — International standard serial number (ISSN)*

[2] ISO 11784:1996, *Radio frequency identification of animals — Code structure*

[3] ISO/IEC 15459 (all parts), *Information technology — Unique identifiers*

[4] ISO/IEC 18004:2006, *Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification*

[5] ISO/IEC 15424:2008, *Information technology — Automatic identification and data capture techniques — Data Carrier Identifiers (including Symbology Identifiers)*

[6] ISO/IEC 15961, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: application interface*

[7] ISO/IEC 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

[8] ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

[9] ISO/IEC 18000-6, *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*

[10] IETF RFC 791, *Internet Protocol*

[11] IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

[12] EPC Tag Data Standard, http://www.gs1.org/gsmp/kc/epcglobal/tds

[13] ITU-T E.164, *The international public telecommunication numbering plan*

[14] ITU-T X.668 (2008) | ISO/IEC 9834-9:2008, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*

[15] ITU-T X.672 | ISO/IEC 29168-1, *Information technology — Open systems interconnection: Object identifier resolution system*

[16] JSR-000257, *Contactless Communication API 1.0*, http://jcp.org/aboutJava/communityprocess/final/jsr257/index.html

ICS 35.040

Price based on 25 pages