INTERNATIONAL STANDARD

ISO/IEC 24791-1

First edition
2010-08-15

Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure —

Part 1: **Architecture**

Technologies de l'information — Identification de radiofréquence (RFID) pour la gestion d'élément — Infrastructure de systèmes logiciels —

Partie 1: Architecture

Reference number
ISO/IEC 24791-1:2010(E)

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 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

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.

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 24791-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

ISO/IEC 24791 consists of the following parts, under the general title *Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure*:

— *Part 1: Architecture*

— *Part 2: Data management*

— *Part 5: Device interface*

The following parts are under preparation:

— *Part 3: Device management*

Introduction

Radio frequency identification (RFID) air interface technology is based on non-contact electro-magnetic communication among interrogators and tags. RFID software systems are composed of RFID interrogators, intermediate software systems, and applications that provide control and coordination of air interface operation, tag information exchange, and health and performance management of system components. RFID technology is expected to increase effectiveness in many aspects of business by further advancing the capabilities of automatic identification and data capture (AIDC). To achieve this goal through the successful adoption of RFID technology into real business environments, RFID devices, software systems, and business applications must provide secure and interoperable services, interfaces, and technologies. This is the goal of ISO/IEC 24791.

Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure —

Part 1:
Architecture

1 Scope

ISO/IEC 24791 defines a Software System Infrastructure that enables RFID system operations between business applications and RFID interrogators. RFID software systems are composed of RFID interrogators, intermediate software systems, and applications that provide control and coordination of air interface operation, tag and sensor information exchange, and health and performance management of system components.

This part of ISO/IEC 24791 provides the following:

- an overview of the Software System Infrastructure;
- the relationship of the Software System Infrastructure to existing ISO components, e.g. ISO/IEC 15962;
- a basic description of each Software System Infrastructure component and the services that it provides (The detailed description of a particular component can be found in other Parts of ISO/IEC 24791.);
- illustrative (informative) deployment models of the components of the Software System Infrastructure.

2 Conformance

This part of ISO/IEC 24791 describes the overall RFID Software System Infrastructure, but it does not define conformance requirements. Conformance requirements are specified in the other parts of ISO/IEC 24791. There is no requirement for an RFID software system to conform to each of the parts; all conformance requirements are based on the individual parts only.

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 19762-1, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 1: General terms relating to AIDC*

ISO/IEC 19762-3, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 3: Radio frequency identification (RFID)*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762-1, ISO/IEC 19762-3 and the following apply.

4.1
component
identifiable part of a larger program or function, typically without reference to the physical computing platform or operating system, that provides specific functionality and might provide or require interfaces to other components

4.2
data management
function and its interfaces that provide reading, writing, collection, filtering, grouping, and event subscription and notification of RFID tag data to higher level applications and interfaces

4.3
device interface
communications interface between an RFID interrogator and upstream clients that provides tag data transfer and control of tag access operations

4.4
device management
protocols and mechanisms that achieve monitoring and control of discovery, configuration, performance and diagnosis of one or more RFID interrogators

4.5
endpoint
one of two components that implements or exposes an interface to other components or uses the interface of another component

4.6
implementation
software and hardware that provides the reduction to practice of a particular function

4.7
interrogator controller
software capability, possibly embodied in a distinct physical device, within the Data Management implementation of the architecture in ISO/IEC 24791-1 which is capable of exercising the data, control and management of interrogators over the device interface defined in ISO/IEC 24791-5

4.8
RFID system
RFID interrogators, intermediate software systems, and applications that provide control and coordination of air interface operation, tag information exchange, and health and performance management of system components

4.9
security
standards-based authentication, authorization, and data privacy appropriate for the specific interface and/or function

5 Abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 19762-1, ISO/IEC 19762-3 and the following apply.

AIDC	automatic identification and data capture
SSI	software system infrastructure
UML	unified modelling language

6 Architecture overview

6.1 General

The Software System Infrastructure architecture consists of standard interface definitions and the implementations in which they exist to provide a particular service or capability. This distinction is necessary to clearly separate the functions which can and should be standardized (the interfaces) from the realization of the interfaces and the product embodiments in which they reside (the implementations). The basic logical relationship among the interfaces and implementations of the Software System Infrastructure is depicted in Figure 1.

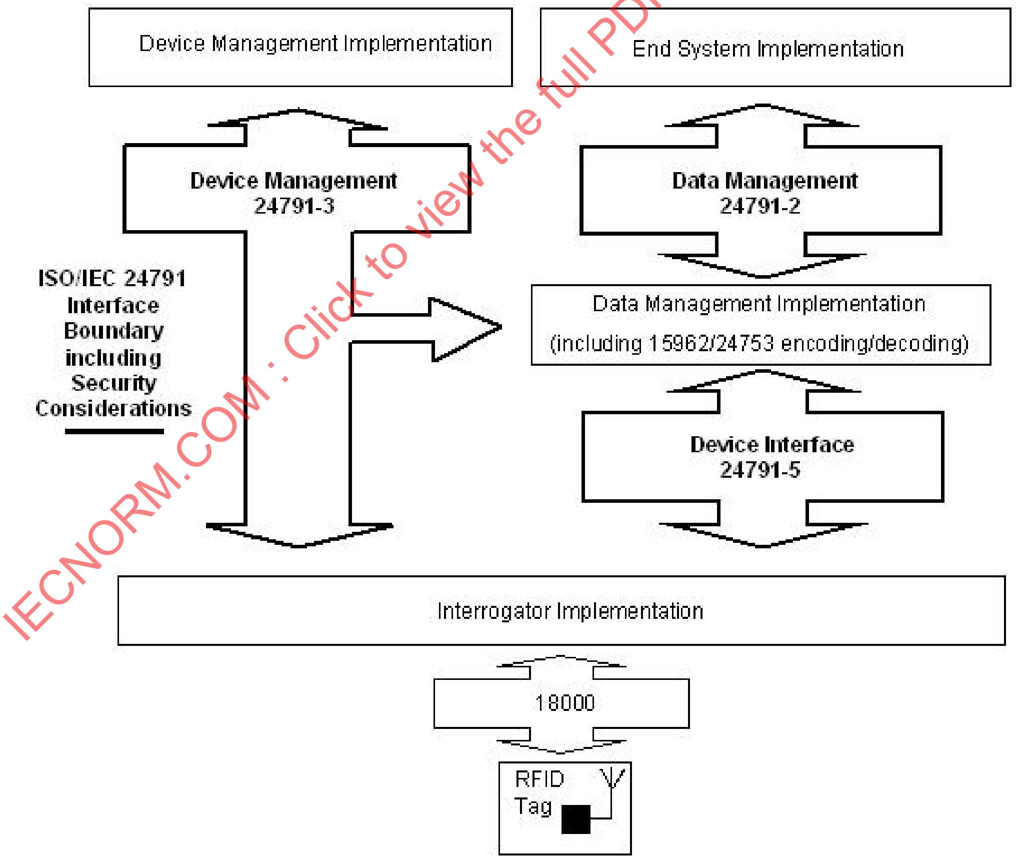
Device Management Implementation
End System Implementation
Device Management
24791-3
Data Management
24791-2
ISO/IEC 24791
Interface
Boundary
including
Security
Considerations
Data Management Implementation
(including 15962/24753 encoding/decoding)
Device Interface
24791-5
Interrogator Implementation
18000
RFID
Tag

Figure 1 — Architecture Overview including Relationships to other RFID Standards

While Figure 1 is intended to show the relationships among the full set of components defined in this architecture, there is no requirement that a particular system, product, or embodiment of this architecture implement all interfaces and implementations defined herein. As specified in Clause 2, the only conformance requirements are those placed upon implementations of the individual Part standards.

The parts of ISO/IEC 24791 that define Data Management, Device Interface, and Device Management each provide one or more interfaces which allow a client to communicate with a service-providing implementation, either within the same computing device or across a network. These client and service implementations are consistently referred to as Client Endpoints and Services Endpoints, respectively, and in general, the Client Endpoint accesses the capabilities provided by the Services Endpoint. It is the responsibility of the specific Part standard to define the formats, procedures, operations, and conformance requirements of each interface.

In addition to defining interfaces for providing configuration and control of the implementations in the network, Device Management may also define requirements for basic initial operation of interrogators, particularly related to initialization in networked environments.

Security considerations provided in each interface specification define how the Parts of ISO/IEC 24791 provide authentication, authorization, and data privacy to protect the implementations from security threats.

6.2 Tag and sensor data considerations

RFID-based AIDC applications had an initial focus reading and writing data specifically in the tag memory. More recently, sensors attached or directly associated with RFID tags have been able to communicate sensor information through specific air protocol commands or memory-mapped reads from the tag memory. This direct relationship between sensor data and RFID air protocol capabilities requires this Software System Infrastructure to support operations for sensor data as well as those for basic tag memory reading and writing operations.

6.3 Data, control, and management functional distinctions

This architecture specification divides the functionality provided by the Software System Infrastructure into data, control, and management functions. This division provides for isolation and specialization of that capability to aid understanding and standardization.

The *data* function is comprised of the operations that transfer tag and sensor data between RFID interrogators and higher level components, which include service applications and data managing entities outside of the SSI. In the process of providing this data, it might be filtered, checked for duplication, grouped, reduced in volume, converted to different formats, or otherwise processed as defined by standard or proprietary requirements. Some or all of these functions may be provided in more than one component, possibly in different ways, as defined in the specific Part of ISO/IEC 24791. The writing of data to RFID tags is also a data function in this architecture. The process of writing data to RFID tags may include event-based operation and format conversion.

The *control* function provides the necessary function to affect changes on a conformant interrogator and tags in order to affect the basic reading or writing operation and state of the tags. This control of the system is often necessary to optimize operation based on constraints of the specific environment. For example, the selection of a single air protocol to be utilized based on specific knowledge of the target or situation could be considered a control operation. Another example consists of RF spectrum optimization that may be done by logic that uses RF environment data gathered logically by the control function. The optimization logic itself is outside the scope of these standards, but the mechanisms to request specific data are provided within the standards. Architecturally, the higher level functions in the architecture have fewer control capabilities than lower levels. Specifically, Data Management exposes fewer control capabilities than are exposed by the Device Interface. This allows for increasing abstraction at the higher layers to facilitate the development of applications that can focus on business processes without the requirement to know or control the specific details of the RF and device environment.

The *management* function defines a core set of operations related to the provisioning, monitoring and configuration of services in the Software System Infrastructure in conjunction with management-specific services exposed by an interrogator. The management function provides an extension mechanism to allow implementations to expose the actual capabilities of an interrogator, which may be over and above the core capabilities defined in this part of ISO/IEC 24791, but in a manner consistent with the standard. The management function does not define management of physical device properties on services endpoints other than on interrogators.

6.4 Relationships to other standards

6.4.1 ISO/IEC 15961

ISO/IEC 15961 Part 1 defines commands and responses for reading and writing data to a tag. Part 2 defines the registration authority, Part 3 the data constructs, and Part 4 the sensor commands and responses. The application commands include arguments that can correctly format the data according to the encoding rules of ISO/IEC 15962. Annex B provides further information concerning the relationship of ISO/IEC 15961 to the SSI architecture.

6.4.2 ISO/IEC 15962

ISO/IEC 15962 specifies the data encoding rules and logical memory functions for encoding and decoding data on tags compliant with particular types and modes defined in ISO/IEC 18000. As such, it provides encoding rules that are part of the data management implementation and resides between the data management and device interface.

6.4.3 ISO/IEC 24753

ISO/IEC 24753 will specify the rules for encoding and decoding sensor data on tags compliant with particular types and modes defined in ISO/IEC 18000. As such, it will provide encoding rules and mechanisms that are part of the data management implementation and will reside between the data management and device interface.

6.4.4 EPCglobal standards

EPCglobal standards are supported as defined in the specific Parts of ISO/IEC 24791.

7 UML modelling

Although Figure 1 provides a general overview of the relationship between the interfaces and implementations in the SSI, Unified Modeling Language (UML) is used in the remainder of the document to graphically represent the organization and operation of the interfaces and implementations in the Software System Infrastructure so that a precise and common understanding of the relationships among the components can be defined.

UML is a very rich language, but for simplicity only the Physical Diagram subset of the language is used to represent the architecture of the Software System Infrastructure. Physical diagrams, comprised of Component Diagrams and Deployment Diagrams, represent the relationships among the functions and the interfaces provided by the SSI architectural elements as well as how these functions might exist in standards compliant solutions, respectively.

Examples of how the interfaces and implementations described in this Software System Infrastructure may be implemented on different computing platforms or different logical environments are provided in Annex A. These examples do not require nor endorse any particular product implementation; they simply serve to illustrate how the components may be split across physical and/or network boundaries. Organizations of components other than as shown in Annex A are possible.

7.1 Component diagrams

In this part of ISO/IEC 24791, UML components are represented as shown in Figure 2. The parts of ISO/IEC 24791 can be represented as one or more components that provide the desired function. When represented as a UML component, no requirements on deployment within specific computing hardware or product implementation are made.

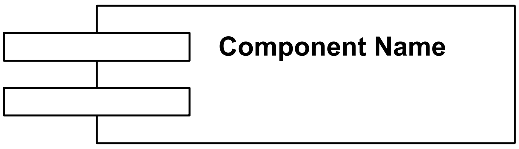

Figure 2 — Component Representation

7.2 Deployment diagrams

Deployment diagrams are used in Annex A to demonstrate example implementation organizations within physical product or computing platforms. In this part of ISO/IEC 24791, these examples are not normative, and other deployment diagrams representing the organization of components would be possible. Figure 3 shows the representation of a node in a deployment diagram in this part of ISO/IEC 24791.

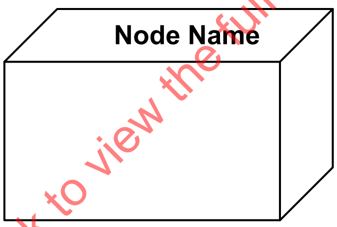

Figure 3 — Node Representation

7.3 Interfaces

Interfaces are represented as shown in Figure 4, with the provider of the service represented by a connection to the straight end of the icon.

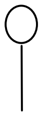

Figure 4 — Interface Representation

7.4 Use

“Use” of an interface or the functions of another component by a component is represented as shown in Figure 5.

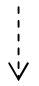

Figure 5 — “Use” Representation

8 Architecture

8.1 Data management

The Data Management component in the Software System Infrastructure provides operations on tag and sensor data including, but not limited to, reading, writing, collection, filtering, grouping, and event subscription and notification. A Data Management component exposes an interface as represented in Figure 6 whereby a Data Management Services Endpoint provides services to one or more Data Management Client Endpoints over an interface binding as will be specified in ISO/IEC 24791-2. The Client and Services Endpoints may exist in a single device or may be accessed across a network.

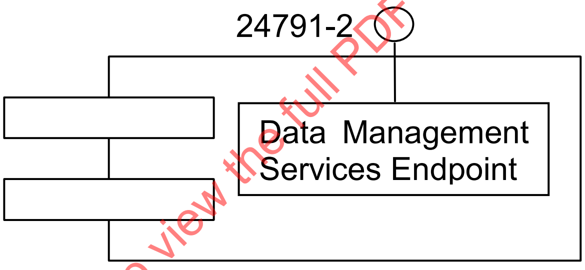

Figure 6 — Data Management Representation

The Data Management services provided to the Client may be synchronous or asynchronous. In the synchronous operation, the services provided by the Services Endpoint happen immediately and synchronously with respect to the request from the Client. Examples of synchronous services are to write the initial data (AFI, DSFID, and/or object id) to a tag by an interrogator module in an RFID printer. In asynchronous operation, a specification of actions to be taken upon a certain condition or state is provided by the Client. This could possibly result in the execution of a complex set of interactions with the tag when the specified condition is encountered. Examples of declarative actions include the ability to write a specific value to all tags with a certain AFI observed by an interrogator.

Data Management provides for transfer of tag and sensor information from a Services Endpoint to a Client Endpoint that requested the specific operation or data. The request for services is considered to be part of the *data* function, and the request is communicated over the interface between the Client and the Services Endpoints. The Services Endpoint processes the Client requests, tag data, and possibly other external inputs (such as time or external logic signal) and delivers the results in the requested form to the Client. In the process of collecting and preparing tag data for delivery to a Client, the Services Endpoint may group, filter, decode, and possibly augment the tag data with additional data. The details of the Services provided by implementations of this component of the architecture will be defined in ISO/IEC 24791-2.

Data Management provides a *control* function that can be utilized by Clients to modify tag access parameters for requested data operations. When requested by a Client, the Data Management Services Endpoint communicates the tag access parameters to the relevant interrogators using either the standard Device Interface or proprietary interrogator interface mechanisms, depending on the specific implementation. There is no architectural requirement for the control functionality to be communicated between Client and Services Endpoints through a single or different communication channel. The specifics of the communication mechanism will be defined in ISO/IEC 24791-2.

The Data Management Interface supports the semantics of tag encoding information as defined in ISO/IEC 15962 including the concepts of the unique identifier, AFI, DSFID, as well as the actual data to be encoded. This interface also supports the semantics of the parameters specified in ISO/IEC 15962 that serve to further define the state of the tag after writing or command execution. Examples of these parameters include those that specify the locking of portions of the tag memory as well as setting the encoding method that is reflected in the DSFID. It is the responsibility of the Data Management Implementation, as shown in Figure 1, to understand a request received from a Data Management Client for a tag data operation, create the ISO/IEC 15962-compliant encoding or tag state request, and communicate this request to the interface or implementation below it in the system.

Data Management will continue to support enhancements to ISO/IEC 15962 that provide additional capacity, performance, and tag format functionality, such as profiles of tag data that minimize the tag operations required to achieve a specific result. Additionally, Data Management will also attempt to provide facilities to support other standardized tag formats in use in RFID software systems. The data format for a particular operation is defined by the Client for an operation requested over the interface between the Data Management Client and the provider of the Data Management Services.

In providing its services, the Data Management Services Endpoint also supports the semantics of sensor data that will be defined in ISO/IEC 24753 with appropriate format decoding capability and support for enhancements to the number and type of sensor information that will be defined in ISO/IEC 24753.

It is not required that an implementation of the Data Management component exist in an implementation of the Software System Infrastructure. The architecture is modular, and it is possible for systems to utilize proprietary or purpose-built applications to provide this function, or for systems to not provide this function at all. Illustrating this point, A.2 and A.3 provide examples of implementations that expose the Data Management interfaces on different platforms, and A.4 shows an implementation of SSI that has no Data Management interface at all.

8.2 Device interface

The Device Interface provides *data* and *control* operation between the Device Interface Services Endpoint on an RFID interrogator and the Client Endpoint typically on a different physical device. It is expected that there will be many RFID interrogators in a system communicating with a smaller number of implementations that provide a Client Endpoint, but all interface operations are described in terms of communication between a single upstream client and a single RFID interrogator. A Device Interface component exposes an interface as represented in Figure 7 whereby a Device Interface Services Endpoint provides services to a Device Interface Client Endpoint over an interface binding as specified in ISO/IEC 24791-5. The Client and Services Endpoints may exist in a single device or may be accessed across a network.

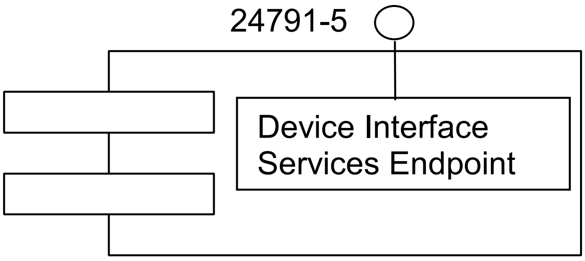

Figure 7 — Device Interface Representation

The Device Interface is responsible for supporting and exercising the capabilities provided by the RFID air protocols to achieve the tag and sensor access goals of an RFID software system. In order to achieve this goal, the standards provided for the data, control, and management functions at this level in the Software System Infrastructure are air-protocol aware and capable of fully exercising specific features of the supported air protocol standards. Equivalently, it is *not* a goal to provide a single, abstract interrogator interface that provides a common interface regardless of the specific air protocol in use. Doing so would reduce the ability of the software systems to access the specific features provided by existing and future air protocols. Note that while the interface commands supporting Type C of ISO/IEC 18000-6 are defined in ISO/IEC 24791-5, additional air protocol support for the SSI Device Interface may be defined in a revision to ISO/IEC 24791-5 or in a different part of ISO/IEC 24791.

The Device Interface supports requests for, and communication of, tag information between the Services Endpoint on RFID interrogators and the Client Endpoint on upstream devices. The data functions include such capabilities such as reading, writing, filtering, and the reporting of tag and sensor data. Synchronous, event-based, and externally triggered operation may be supported for access requests.

The control functions in the architecture provide an interface for the Device Interface Client to exercise specific control over the access operations on an interrogator. This control is specific to each air protocol and is intended to provide the necessary capabilities to allow for software system, interrogator, and RF environment optimization. The control function of the Device Interface also supports the delivery of system, interrogator, tag, and RF environment data from the Services Endpoint to the Client Endpoint. This data can be used by implementations to provide the control required to achieve the desired system goals.

In order to provide an interface that can provide the lowest level of control and data access across the set of supported air protocols and interrogator capabilities, the full encoding and decoding of ISO/IEC 15962 tag and ISO/IEC 24753 sensor data for writing and reading, respectively, is performed above the Device Interface Client in this architecture, as shown in Figure 1. It is the responsibility of the Data Management Implementation to use the services of an ISO/IEC 15962 and/or ISO/IEC 24753 encoder/decoder to format the input for or decode the output from the Device Interface Client as appropriate for the air protocol.

It is important to note that while the architecture supports the ability to achieve a high level of control of an RFID software system, no requirements are placed on an implementation to exercise any specific level of control. The goal of the Device Interface is to provide a Client with the ability to retrieve desired RFID system information from interrogators and request desired tag access actions. The logic that utilizes the Device Interface from an implementation is outside the scope of ISO/IEC 24791-5.

It is not required that an implementation of the Device Interface component exist in an implementation of the Software System Infrastructure. The architecture is modular, and it is possible for systems to utilize proprietary or purpose-built interfaces to interrogators, either across networks or in directly connected configurations. A.2 and A.4 provide deployment examples of interrogators exposing the Device Interface and A.3 shows a deployment whereby an interrogator exposes a Data Management interface and *not* a Device Interface.

8.3 Device management

Device Management defines the interface(s) that provide discovery, provisioning, image management, configuration, performance monitoring, and problem diagnosis of Software System Infrastructure components and interrogators. Device Management also defines a set of standardized operational procedures that shall be executed by conforming devices, typically related to the initial operation of a device in a networked environment.

Specific interface capabilities are provided by a Device Management Services Endpoint. A Device Management Client Endpoint accesses the Services Endpoint in a component that provides the desired service(s). Figure 8 provides the representation of the Device Management interface in a component:

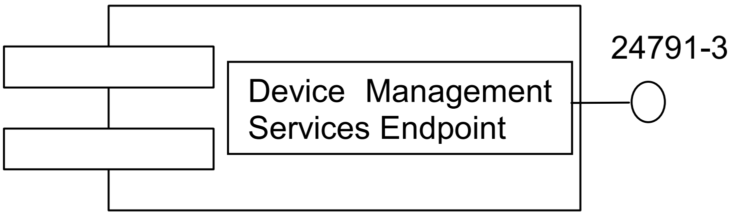

Figure 8 — Device Management Representation

As indicated, this interface is distinct from the data and control interfaces provided by other parts of ISO/IEC 24791. It is possible that the implementation of the Device Management interface utilizes the same network interface as the implementation of one of the data and/or control interfaces in the implementation.

Summaries of the services supported for each component in the architecture are specified below, and full details of the interface protocol(s) the provided management services will be specified in ISO/IEC 24791-3.

The functions covered by Device Management may be grouped as follows:

- *Discovery:* the process of automatically finding components and devices in a system as well as dynamically identifying Service Endpoints and enabling connections between the components and services.

- *Configuration:* the process of setting operational parameters for components that are loaded at system initialization and that change relatively infrequently, primarily through user interaction.

- *Initialization:* the process of providing initial deployment of network and operating parameters for interrogators as well as installing, updating, maintaining software images at desired versions through a dynamic, potentially automated process.

- *Monitoring:* the gathering of statistics and state data useful for determining the historic and current operational state of a component, in particular an interrogator or an SSI component that provides a Data Management implementation function, such as an interrogator controller within the Data Management implementation depicted in Figure 1.

- *Diagnostics:* the mechanism to aid in the detection and isolation of faults or abnormal operation within a component of the Software System Infrastructure. Where the diagnostics involve the computing platform, they are applicable to an interrogator only. Diagnostic capabilities may be defined for other SSI software components, but diagnostic capabilities for general purpose computing platforms will not be defined.

The interfaces that will be defined in ISO/IEC 24791-3 will provide extension mechanisms to allow implementations to expose management services beyond those specifically defined in the standard. This is consistent with standards-based approaches currently used in the management of telecommunication devices.

It is important to note that not all of the above capabilities are required to be deployed in all implementations of a Device Management Services Endpoint. For example, interrogators may implement and expose a different set of ISO/IEC 24791-3 capabilities from interrogator controllers. Furthermore, different classes of interrogators may implement and expose different sets of ISO/IEC 24791-3 capabilities. Conformance requirements for implementations of the Device Management Services Endpoint will be defined in ISO/IEC 24791-3. A.5 and A.6 illustrate different organizations of interrogators and an interrogator controller that expose the Device Management interface.

8.4 Security considerations

The Parts of ISO/IEC 24791 that define interfaces include recommendations and requirements for security between the Client Endpoint and the Services Endpoint. The Parts of ISO/IEC 24791 that define interfaces are:

- ISO/IEC 24791-2, Data Management
- ISO/IEC 24791-3, Device Management
- ISO/IEC 24791-5, Device Interface

Security mechanisms for RFID air interface operation are specifically outside the scope of this specification. However, certain aspects of RFID air interface security such as passwords may need to be supported by the SSI. These requirements will be specifically identified and supported in the relevant standards of ISO/IEC 24791.

Annex A
(informative)

Implementation examples

A.1 General

This part of ISO/IEC 24791 specifies the operation of RFID software systems between end user applications and the physical hardware that implements the RFID air interface protocols. There are many possible organizations of the software components defined by this part of ISO/IEC 24791, including how the components are distributed among different physical computing platforms. The different platforms on which the components may reside are represented in the following sections of this annex as individual UML *nodes* in a deployment diagram.

Note that the communication with RFID tags over the air interface is beyond the scope of this part of ISO/IEC 24791; therefore, RFID tags, sensors, and the ISO/IEC 18000 series tag air protocol interfaces are not represented in the following figures. They should be assumed to be "below" the interrogators in the diagrams, with both the interrogators and the tags properly implementing the ISO/IEC 18000 series air protocol operations.

A.2 Interrogator Controller with Interrogator Deployment

In the example illustrated in Figure A.1, end user applications that require RFID data or sensor operations communicate with a network-based interrogator controller node using a Data Management Client Endpoint. The interrogator controller implements the Client Endpoint of the Device Interface to communicate with and control a number of RFID interrogators that implement the Device Interface Services Endpoint. In deployments such as this, it is possible that multiple applications will be communicating with multiple interrogator controllers, which in turn, may communicate with multiple RFID interrogators.

In this example deployment, the interrogator controller node provides the RF control and data management functions for a potentially large number of interrogators in the RFID system, while also providing tag and sensor data to more than one client and/or application in the system. This style of deployment allows the end user applications to access tag and sensor data in the RFID system without being required to attempt control of the details of the RF system.

The interrogator controller provides the Data Management Services Endpoint as well as implementation-specific logic that collects, transforms, and presents the data to the Data Management interface. The process of managing this data may require the use of an ISO/IEC 15962 encoding/decoding function as it creates and processes data and/or requests.

The interrogators in this deployment model process the requests from the Device Interface Client Endpoint on the interrogator controller in a Device Interface Services Endpoint. These requests may be synchronous or asynchronous in nature, with either synchronous or asynchronous responses respectively. The operations requested over the Device Interface may be for any supported air protocol at any time, and the interrogator will provide the proper air protocol operation based on the Device Interface request.

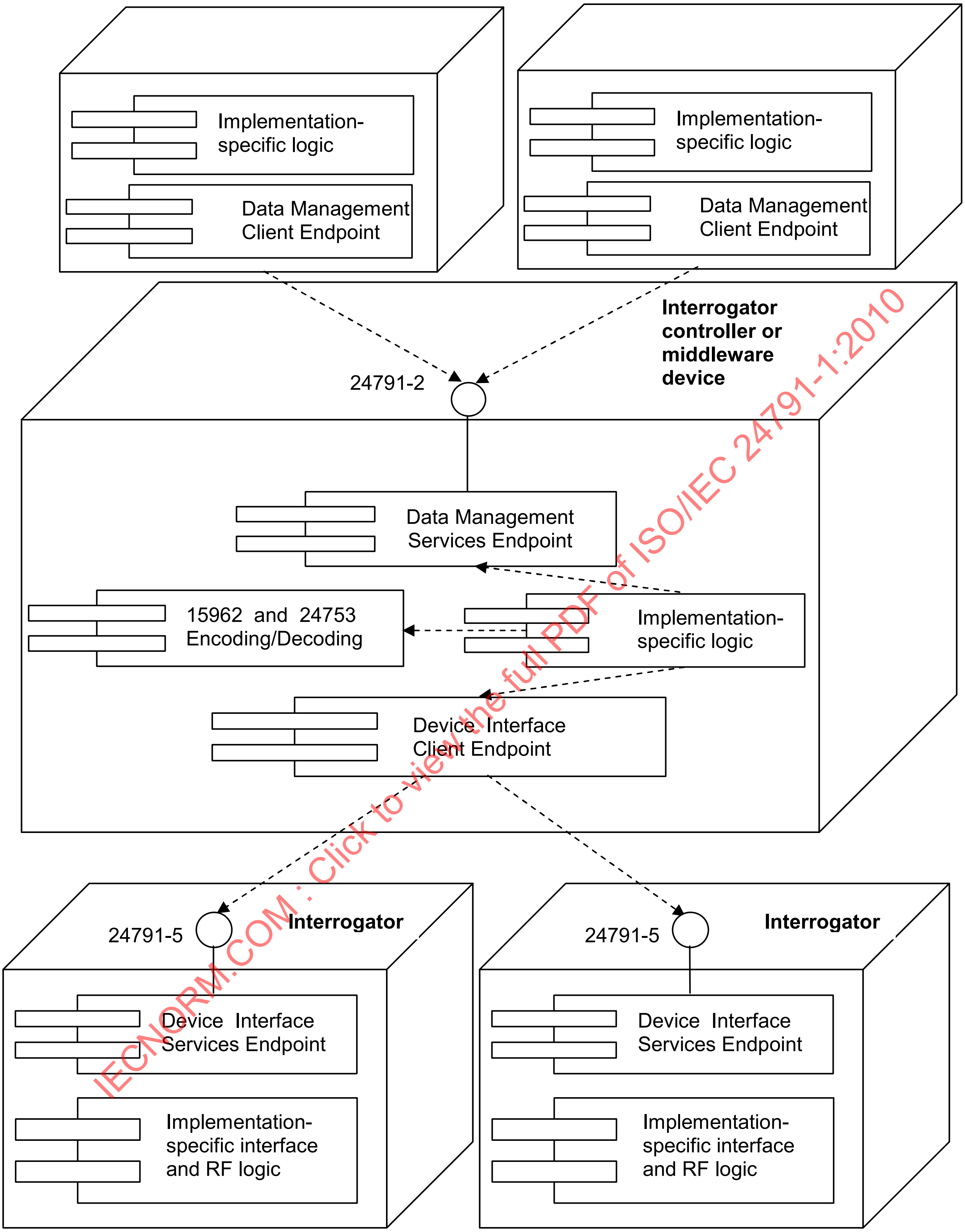
Implementation-specific logic
Data Management Client Endpoint
Implementation-specific logic
Data Management Client Endpoint
Interrogator controller or middleware device
24791-2
Data Management Services Endpoint
15962 and 24753 Encoding/Decoding
Implementation-specific logic
Device Interface Client Endpoint
24791-5
Interrogator
Device Interface Services Endpoint
Implementation-specific interface and RF logic
24791-5
Interrogator
Device Interface Services Endpoint
Implementation-specific interface and RF logic

Figure A.1 — Node Diagram with Interrogator Controller and Interrogators

A.3 Interrogators Exposing Data Management Interface

In Figure A.2, RFID interrogators provide a Data Management Services Endpoint to directly support requests for tag and sensor data from Data Management Client Endpoints in end user applications. In these deployments, the specific control of RFID system parameters across interrogators is either not required or is implemented through interrogator procedures outside the scope of this part of ISO/IEC 24791.

The interrogator provides the Data Management Services Endpoint as well as implementing specific logic that collects, transforms, and presents the data to the Data Management interface. The process of managing this data may require the use of an ISO/IEC 15962 encoding/decoding function as it creates and processes data and/or requests.

Unlike the previous deployment example, there is no Device Interface exposed in this scenario. The interrogator processes the requests from the Data Management interface and interacts directly with its implementation-specific RF functions to perform the desired operations.

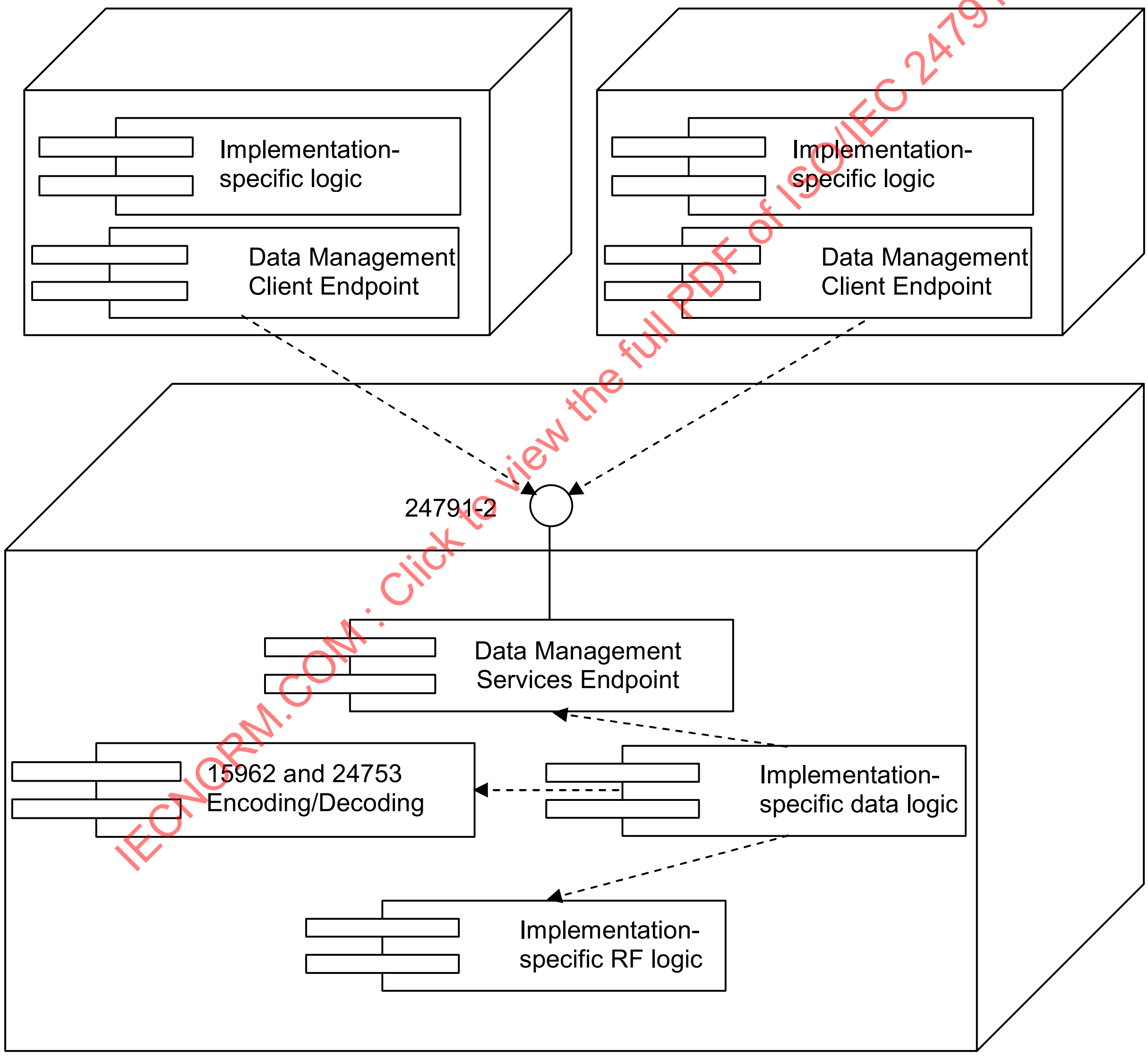
Implementation-specific logic
Data Management Client Endpoint
Implementation-specific logic
Data Management Client Endpoint
24791-2
Data Management Services Endpoint
15962 and 24753 Encoding/Decoding
Implementation-specific data logic
Implementation-specific RF logic

Figure A.2 — Node Diagram with Interrogator-based Data Management