INTERNATIONAL STANDARD

ISO/IEC 24791-3

First edition
2014-03-01

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

Part 3: Device management

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

Partie 3: Gestion de dispositif

Reference number
ISO/IEC 24791-3:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

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 24791-3 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 3: Device management*
- *Part 5: Device interface*

Introduction

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 the standards defined for RFID Software System Infrastructure (SSI), ISO/IEC 24791.

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

Part 3: Device management

1 Scope

This part of ISO/IEC 24791 defines interfaces for device management of RFID systems. Interfaces are defined that provide for discovery, configuration, initialization and monitoring of RFID systems within the Software System Infrastructure (SSI).

This standard only deals with devices that provide RFID related services. It does not distinguish the form factor of such RFID devices.

This part of ISO/IEC 24791 provides two distinct *interface sets*, one based on the EPCglobal Discovery, Configuration, and Initialization (DCI) standard and the IETF SNMP RFCs and the other based on the Organization for the Advancement of Structured Information Standards (OASIS) Device Profile for Web Services (DPWS) standard. The definition of the Device Profile for RFID will be referred to in this part as the RFID Device Management Profile, or RDMP.

Each interface option set provides interface definitions that provide ISO/IEC 24791-3 Client Endpoints and Services Endpoints with the mechanisms for:

- discovery of the RFID devices and services on a local or remote subnet
- a firmware upgrade service
- a management service that implements configuration related functions
- a monitoring service for reporting alerts, diagnostics, and performance information.

The two interface set definitions provided by this part of ISO/IEC 24791 allow for clients and services endpoints to implement and provide the services based on the specific characteristics of the RFID system to be implemented. Clause 2 defines the Conformance requirements for systems that implement components of one or both of the interface sets.

2 Conformance

This part of ISO/IEC 24791 provides two interface sets; the DCI and SNMP Interface Set and the RDMP interface Set. If a certain implementation conforms to the mandatory functions of at least one of the interface sets, that implementation is conformant to this part of ISO/IEC 24791.

2.1 DCI and SNMP Interface Set

This version of this International Standard divides the DCI capabilities into two *Conformance Groups:*

- Discovery, Configuration, and Initialization Conformance Group

This Conformance Group is defined in Clause 8.2.1. It specifies the protocols and operational procedures that are required for conforming Interrogator Implementations and Device Management Implementations, as defined in this part of ISO/IEC 24791 as well as in ISO/IEC 24791-1.

- Performance Monitoring and Diagnostics Conformance Group

  This Conformance Group is defined in Clause 8.2.2. It specifies the SNMP MIBs that may be implemented by Interrogator Implementations and Data Management Implementations as defined in this part of ISO/IEC 24791 as well as in ISO/IEC 24791-1. Conforming implementations claim conformance to the MODULE_COMPLIANCE statements in the SNMP MIBs appropriate for the particular implementation.

A conforming implementation must implement all of the requirements of each Conformance Group for its particular function in the SSI, but an implementation is not required to claim conformance to either group.

2.2 RDMP Interface Set

This version of the International standard specifies the following device management capabilities in RDMP

- Discovery of devices and hosted services in devices
- A Firmware Upgrade Service to initialize and manage firmware on devices
- A Management service to set and get device configuration and to perform specific device operations, such as reboot
- A monitoring service to monitor the health of a device using events and statistics

A conforming RDMP implementation shall implement DEVICE as defined in DPWS

A conforming RDMP implementation may implement the firmware update service (FUS). If it does implement FUS, it shall implement the mandatory requirements of the firmware update service

A conforming RDMP implementation may implement the management service (MS). If it does implement MS, it shall implement the mandatory requirements of the management service.

A conforming RDMP implementation may implement the monitoring service (MNS). If it does implement MNS, it shall implement the mandatory requirements of the monitoring service.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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)*

ISO/IEC 24791-5, *Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure — Part 5: Device interface*

Devices Profile for Web Services Version 1.1, OASIS Standard July 2009- http://docs.oasis-open.org/ws-dd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.pdf.

Control and Provisioning of Wireless Access Points - Protocol Specification - http://www.rfc-editor.org/rfc/rfc5415.txt

EPCglobal, Reader Management Standard, http://www.epcglobalinc.org/standards/rm.

EPCglobal, Discovery, Configuration, & Initialisation Standard for Reader Operations, http://www.epcglobalinc.org/standards/dci.

Internet Engineering Task Force, RFC3418 - Simple Network Management Protocol (SNMP), http://www.faqs.org/rfcs/rfc3418.html

Internet Engineering Task Force, RFC 2011 – SNMPv2 Management Information Base for the Internet Protocol using SMIv2, http://www.faqs.org/rfcs/rfc2011.html

Internet Engineering Task Force, RFC 2863 – The Interfaces Group MIB, http://www.faqs.org/rfcs/rfc2863.html

XML Schema Part 2: Datatypes: http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/

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 that provides specific functionality

4.2
Device
RFID Interrogator implementation

4.3
Interface
functions or mechanisms that provide communications to or from a component

4.4
Data management
device functionality that includes or is a combination of reading, writing, collection, filtering, grouping, and event subscription and notification of RFID tag data to higher level applications and interfaces

4.5
Device management
functionality that includes or is a combination of monitoring and control of discovery, configuration, performance and diagnosis of one or more RFID interrogators

4.6
Endpoint
component that implements or exposes an interface to other components or uses the interface of another component

4.7
Implementation
software and hardware that provides the reduction to practice of particular functionality

4.8
Interrogator controller
software capability possibly embodied in a distinct physical device, within the Data Management implementation of the architecture in ISO/IEC 24791-1 and capable of exercising the data, control, and management of interrogators over the device interface defined in ISO/IEC 24791-5

4.9
CLIENT
network endpoint that sends MESSAGEs to and/or receives MESSAGEs from a SERVICE.

4.10
SERVICE
software system that exposes its capabilities by receiving and/or sending MESSAGEs on one or several network endpoints.

4.11
DEVICE
distinguished type of SERVICE that hosts other SERVICEs and sends and/or receives one or more specific types of MESSAGEs.

4.12
HOSTED SERVICE
distinguished type of SERVICE that is hosted by another SERVICE. The lifetime of the HOSTED SERVICE is a subset of the lifetime of its host. The HOSTED SERVICE is visible (not encapsulated) and is addressed separately from its host. Each HOSTED SERVICE has exactly one host. (The relationship is not transitive.)

5 Symbols and 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.

AC	Access Controller
DCI	EPCglobal Discovery, Configuration, Initialization Standard
DPWS	Devices Profile for Web Services Standard
IETF	Internet Engineering Task Force
RFC	Request For Comment
RM	Reader Management
SNMP	Simple Network Management Protocol
SSI	Software System Infrastructure
UML	Unified Modelling Language
FUS	RDMP Firmware Update Service
MS	RDMP Management Service
MNS	RDMP Monitoring Service

6 Software System Infrastructure Architecture Overview

ISO/IEC 24791-1 defines the architecture for the Software System Infrastructure. The basic relationship among the interfaces and implementations of the Software System Infrastructure is depicted in Figure 1.

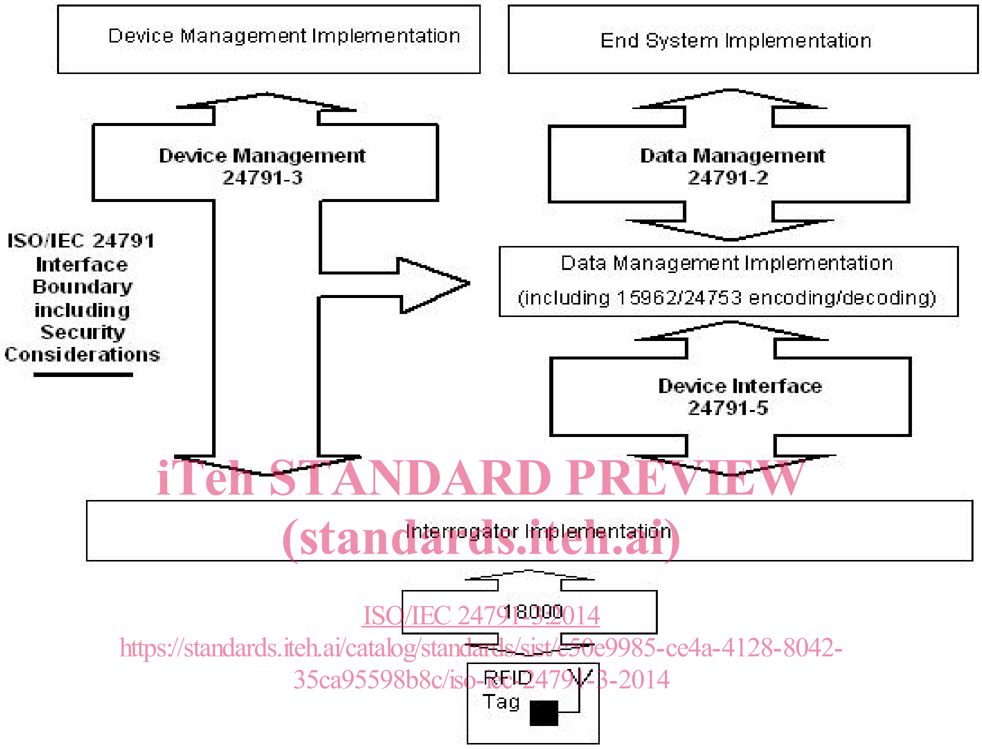
Device Management Implementation
End System Implementation
Device Management
24791-3
Data Management
24791-2
ISO/IEC 24791
Interface
Boundary
including
Security
Considerations
Data Management Implementation
(including 15962/24753 encoding/decoding)
Device Interface
24791-5
Interrogator Implementation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

Figure 1 — Architecture Overview including Relationships to Other RFID Standards

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 standard to define the formats, procedures, operations, and conformance requirements of each interface.

Device Management is concerned with providing discovery, configuration, initialization, performance monitoring, and diagnostics of Software System Infrastructure components and interrogators. As shown in Figure 1, Device Management defines *interfaces* that provide pairwise communications between Interrogator implementations, Data Management implementations, and Device Management Implementations.

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. This is necessary in order to achieve the SSI goal of providing scalable deployment and management of large numbers of interrogators in a system.

Although Figure 1 depicts the Device Management Implementation residing outside of the boundary of the SSI, the Device Management Implementation may be implemented within any device in a system. For example, it may reside within a standalone network management application or it may be just one component within a device that is also providing a Data Management Implementation. It may also be one component of an application that is also providing the End System Implementation. As with all other components of the SSI as defined in ISO/IEC 24791 Part 1, the platform on which the standard interfaces are implemented is not important; it is conformance to the interfaces and procedures defined in the ISO/IEC 24791 that is important. Examples of different deployment models of this part of ISO/IEC 24791 are provided in Annex A.

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 for the figures in this document to graphically represent the organization and operation of the Device Management interfaces and implementations 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. Refer to ISO/IEC 24791-1 for a more complete description how UML is used in the part standards of 24791.

8 Device Management

8.1 Architecture

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

Specific Device Management 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 2 provides the representation of the Device Management interface in a component:

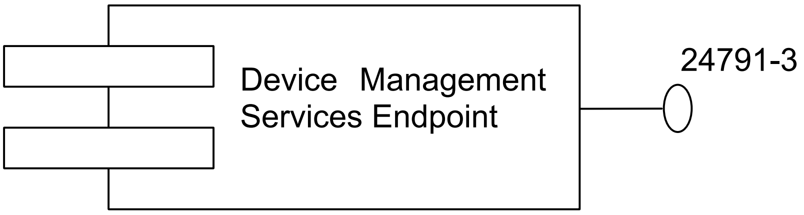

Figure 2 — Device Management Representation

The software programs that provide Device Management Client and Services Endpoints may reside within any of the Implementations that may exist in the SSI, as shown in Figure 1. This part of ISO/IEC 24791 does define requirements on the how the implementations are developed or packaged within computing or network platforms; requirements are only defined for the operation that is provided.

Device Management 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. It is also possible that for a specific operation or interface, a component may be both a Client and Services Endpoint, essentially resulting in peer-to-peer operation or a negotiated Client/Server relationship. This does not change the architecture defined in this part of ISO/IEC 24791 or in ISO/IEC 24791-1.

The functions covered by Device Management may be grouped and defined 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 defined by this International Standard will provide extension mechanisms to allow implementations to expose management services beyond those specifically defined in this 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 Data Management Implementations. 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 are defined in Clause 2.

9 DCI and SNMP Interface Set

9.1 Discovery, Configuration, and Intialization Conformance Group

9.1.1 General

Conforming devices implement discovery, configuration, and initialization capabilities through the implementation of the protocols and procedures defined in this Conformance Group. This subclause of this International Standard references the EPCglobal Discovery, Configuration, and Initialization (DCI) for Reader Operations standard for the normative requirements for this SSI capability. The EPCglobal DCI standard, references the IETF CAPWAP (Configuration and Provisioning for Wireless Access Points) standard for the core network protocol, security, and communication operations and interfaces.

9.1.2 Interrogator Implementations

Interrogators that conform to this International Standard for discovery, configuration, and initialization capabilities shall implement all requirements, indicated with “shall”, for the *Reader* function as defined in the EPCglobal DCI standard. Conforming implementations may implement any requirements for the Reader function indicated with “may” in the EPCglobal DCI standard.

9.1.3 Device Management Implementations

Device Management Implementations that conform to this part of ISO/IEC 24791 shall implement all requirements, indicated with "shall" for the Access Controller (AC) function as specified in the EPCglobal DCI standard. Conforming implementations may implement any requirements indicated with "may" in the EPCglobal DCI standard.

It is not required that implementations of the Access Controller also implement the *RO Client* function, which is equivalent to the ISO/IEC 24791-5 Device Interface Client functionality, although it is possible and likely that the implementations will be co-resident in computing or network systems. Note that in such cases, the Device Management Implementation and Data Management Implementation from Figure 1 will coexist in the same device. This example is demonstrated in Annex A.

9.2 Performance Monitoring and Diagnostics Conformance Group

9.2.1 General

Performance monitoring and diagnostic information access within of SSI components is provided by Device Management Services Endpoints that expose SNMP MIBs within one or more of the implementations defined in ISO/IEC 24791-1 and illustrated in Figure 1 of this International Standard. SNMP clients (Client Endpoints in the SSI architecture) access the exposed device management information using the Simple Network Management Protocol (SNMP). Implementations claim conformance to one or more MODULE_COMPLIANCE statements within the specific SNMP MIBs normatively referenced in the following subclauses.

Conformance requirements for implementations that expose an SNMP MIB for performance monitoring and diagnostic information access according to this International Standard are defined in the following subclauses. It is not required that an implementation implement or claim conformance to both of the following subclauses if it claims conformance to one of them.

9.2.2 Interrogator Implementations

The EPCglobal Reader Management specification Version 1.0.1 defines an SNMP MIB for performance monitoring and diagnostic information access for Interrogator Implementations.

The MIB groups specified as MANDATORY-GROUPS in the SNMP MODULE-COMPLIANCE statement referenced in the EPCglobal Reader Management Version 1.0.1 specfication shall be implemented by interrogators that claim conformance to this subclause of this International Standard.

Implementation of non-SNMP bindings or transports described in the EPCglobal Reader Management standard is not required by this International Standard.

In addition, the network-attached devices in which the interrogator implementations execute shall implement:

1. The MIB-II System Group, defined in the SNMPv2-MIB module in RFC 3418

2. The MIB-II IP Group, defined in the IP-MIB module in RFC 2011

3. The MIB-II Interfaces Group, defined in the IF-MIB in RFC 2863

9.2.3 Data Management Implementations providing Interrogator Controller Functionality

Annex B of this International Standard provides an SNMP MIB for performance monitoring and diagnostic information access of Data Management Implementations that implement a Device Interface (ISO/IEC 24791-5) Client Endpoint for the control and data access of interrogators. These implementations have been defined as *interrogator controllers*.

The MIB groups specified as MANDATORY-GROUPS in the SNMP MODULE-COMPLIANCE statement in Annex B of this International Standard shall be implemented by interrogator controller functions within Data Management Implementations that claim conformance to this subclause of this document. Note that other functions that may be implemented by a Data Management Implementation, such as the Data Management Services Endpoint, may provide performance monitoring and diagnostic information access by additions the the MIB in Annex B in a future version of this International Standard.

In addition, the network-attached devices in which the data management implementations execute shall implement:

1. The MIB-II System Group, defined in the SNMPv2-MIB module in RFC 3418
2. The MIB-II IP Group, defined in the IP-MIB module in RFC 2011
3. The MIB-II Interfaces Group, defined in the IF-MIB in RFC 2863

10 RDMP Interface Set

10.1 Non Normative Text

Non normative text is formatted as below in the RDMP Interface set.

```
This is non normative text
```

NOTE the Project Editor is aware that this clause 8.3.1 is both incorrect and redundant, now that the text has been reformatted to follow ISO drafting rules for non-normative Notes. During the next ballot, the Project Editor will submit a PE comment to remove this subclause 8.3.1 and renumber the subsequent subclauses.

10.2 XML Namespace

In addition to the namespaces defined in DPWS, this standard defines the following XML namespace.

http://standards.iso.org/iso/24791/-3/2013/01/rdmp

Table 1 lists XML namespaces that are used in this specification. The choice of any namespace prefix is arbitrary and not semantically significant.

Prefix	XML Namespace	Specification(s)
rdmp	http://standards.iso.org/iso/24791/-3/2013/01/rdmp	This specification
dpws	http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01	DPWS
soap	http://www.w3.org/2003/05/soap-envelope	See DPWS
wsa	http://www.w3.org/2005/08/addressing	See DPWS

Table 1 — XML Namespaces

10.3 Device Discovery

A conformant RDMP device shall implement DEVICE, as defined in DPWS.

A conformant RDMP device shall advertise the rdmp: ISO/IEC 24791-3 type in discovery messages.