BS ISO/IEC 24791-3:2014

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 24791-3:2014

## National foreword

This British Standard is the UK implementation of ISO/IEC 24791-3:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 73031 3

ICS 35.040

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

**Amendments issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24791-3:2014

# 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)

Documents
Document Sharing Hub

© ISO/IEC 2014

Full document details: BS ISO/IEC 24791-3:2014

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland



© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24791-3:2014

# Contents

Page

**Foreword** ..... iv

**Introduction** ..... v

**1 Scope** ..... 1

**2 Conformance** ..... 1
**2.1 DCI and SNMP Interface Set** ..... 1
**2.2 RDMP Interface Set** ..... 2

**3 Normative references** ..... 2

**4 Terms and definitions** ..... 3

**5 Symbols and abbreviated terms** ..... 4

**6 Software System Infrastructure Architecture Overview** ..... 5

**7 UML Modelling** ..... 6

**8 Device Management** ..... 6
**8.1 Architecture** ..... 6

**9 DCI and SNMP Interface Set** ..... 7
**9.1 Discovery, Configuration, and Intialization Conformance Group** ..... 7
**9.2 Performance Monitoring and Diagnostics Conformance Group** ..... 8

**10 RDMP Interface Set** ..... 9
**10.1 Non Normative Text** ..... 9
**10.2 XML Namespace** ..... 9
**10.3 Device Discovery** ..... 9
**10.4 Device Metadata** ..... 10
**10.5 Firmware Update Service** ..... 11
**10.6 Management Service (MS)** ..... 18
**10.7 Operation Error Reporting** ..... 28
**10.8 Monitoring Service (MNS)** ..... 29
**10.9 Security** ..... 33
**10.10 Extensibility** ..... 34

**Annex A** (informative) **Implementation Examples** ..... 36

**Annex B** (normative) **SSI Device Management MIB** ..... 39

**Annex C** (normative) **RDMP WSDLs and XSDs** ..... 48

**Bibliography** ..... 80

© ISO/IEC 2014 – All rights reserved


Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

# 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*


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

## 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.

© ISO/IEC 2014 – All rights reserved


Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24791-3:2014

# 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

© ISO/IEC 2014 – All rights reserved



Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24791-3:2014

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.


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

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

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

**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


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

## 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.

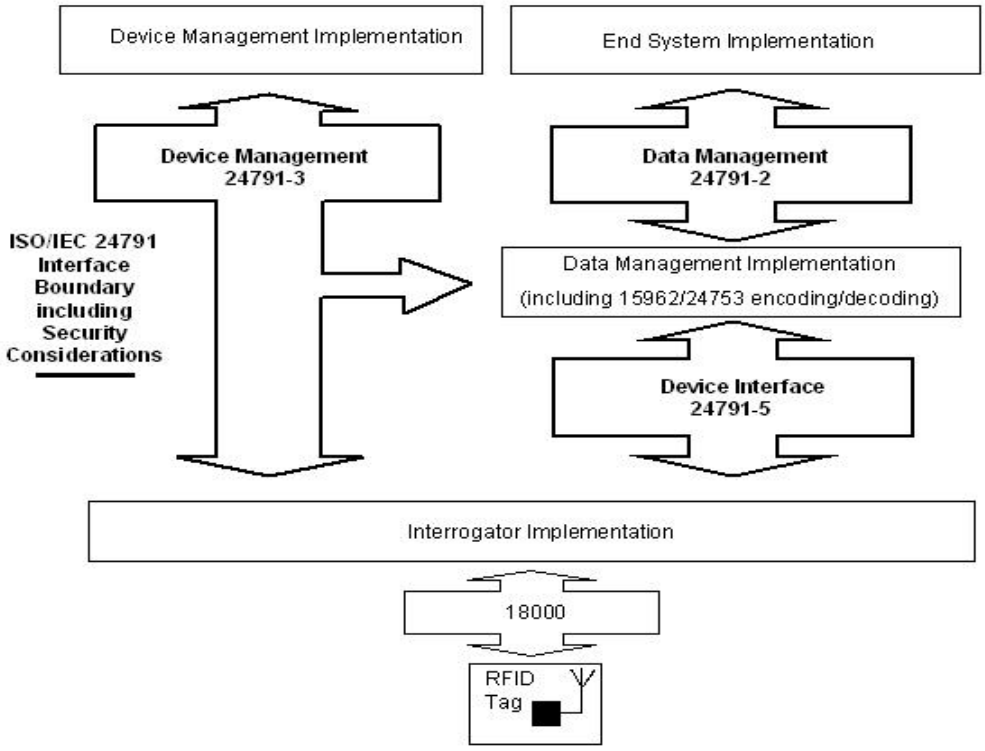


**Figure 1 — Architecture Overview including Relationships to Other RFID Standards**

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.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

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


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

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.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

### 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*.


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

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.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

NOTE DPWS uses WS-Discovery as the device discovery protocol. WS-Discovery defines a multicast discovery protocol. To be discovered by RDMP clients, RDMP devices should implement WS-Discovery as per the requirements of DPWS and as per the additional type requirement defined above. In summary, a RDMP device that implements DEVICE would include dpws:device and rdmp:ISO24791-3 in the Types section of the hello and probe match messages. A transport address may be sent by a device in the hello and probe match messages.

## 10.4 Device Metadata

### 10.4.1 General

This part of ISO/IEC 24791 does not specify requirements for exchanging device metadata in addition to those already specified in DPWS.

NOTE 1 DPWS defines a standard mechanism for retrieving device metadata from a device. Metadata would include information such as manufacturer name, model name, firmware version etc. This mechanism is documented in the Description Section in the DPWS spec. We describe it briefly here for illustration.

NOTE 2 An RDMP client interested in getting metadata about a RDMP device would send a SOAP envelope containing a WS-Transfer Get message to the transport address of the chosen device. The RDMP device would then send a WS-Transfer GetResponse message containing the device metadata.

NOTE 3 Please refer to the DPWS specification, section titled **Description** for more details and requirements.

### 10.4.2 Service Discovery

An RDMP conformant device may advertise services that are not specified in this standard in the dpws:Relationship/dpws:Host/dpws:Types

NOTE 1 In addition to device discovery, DPWS specifies mechanisms for discovery of HOSTED SERVICES on a device. Some examples of HOSTED SERVICES are a stock quote service, firmware update service, a print service, a calendar service etc. An RDMP client discovers a HOSTED service by parsing the Metadata section of the WS-Transfer GetResponse.

An example response that advertises a Printer Service is below:

```
<?xml version="1.0" encoding="utf-8"?>
<wsoap12:Envelope
      xmlns:wsoap12="http://www.w3.org/2003/05/soap-envelope"
      xmlns:mex="http://schemas.xmlsoap.org/ws/2004/09/mex"
      xmlns:wsa="http://www.w3.org/2005/08/addressing"
      xmlns:dpws="http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01"
>
...
<mex:MetadataSection
Dialect="http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01/Relationship">
    <dpws:Relationship Type="http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01/host">
          <dpws:Hosted>
                <wsa:EndpointReference>
                      <wsa:Address>
      http://192.168.0.101:80/SamplePrintService0
                      </wsa:Address>
                </wsa:EndpointReference>
                <dpws:Types
                      xmlns:spt="http://example.com/wsdp/sample/print">
                      spt:PrinterServiceType
                </dpws:Types>
                <dpws:ServiceId>
```


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

```
                    http://example.com/sample/print/PrintService
                </dpws:ServiceId>
            </dpws:Hosted>
        </dpws:Relationship>
</mex:MetadataSection>
</wsoap12:Envelope>
```

**An example for advertising ISOIEC24791-5 (LLRP) service by RDMP devices:-**

```
<mex:MetadataSection
Dialect="http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01/Relationship">
    <dpws:Relationship Type="http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01/host">
            <dpws:Hosted>
                <wsa:EndpointReference>
                    <wsa:Address>                                                    ISOIEC24791-
5://192.168.0.101:5084/                    </wsa:Address>
                </wsa:EndpointReference>
                <dpws:Types
                    ISOIEC24791-5
                </dpws:Types>
                <dpws:ServiceId>
                    http://example.com/sample/ISO24791-5/
                </dpws:ServiceId>
            </dpws:Hosted>
        </dpws:Relationship>
</mex:MetadataSection>
```

NOTE 2 Note that, the types sent in the dpws:Relationship/dpws:Host/dpws:Types element are the portTypes of services that are supported by this device. In contrast, the types element in WS-Discovery messages contains discovery-layer portTypes that are implemented by the device.

## 10.5 Firmware Update Service

### 10.5.1 General

This part of ISO/IEC 24791 describes a Firmware Update Service that is used to initialize and update firmware for RFID devices. The client is responsible for initiating a firmware update. The device downloads the firmware from the location presented by the client.

### 10.5.2 Firmware Update Service state machine

The Firmware Update Service on the device shall maintain the states as described in the firmware update state machine. Figure 3 illustrates the state machine for a firmware update service.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

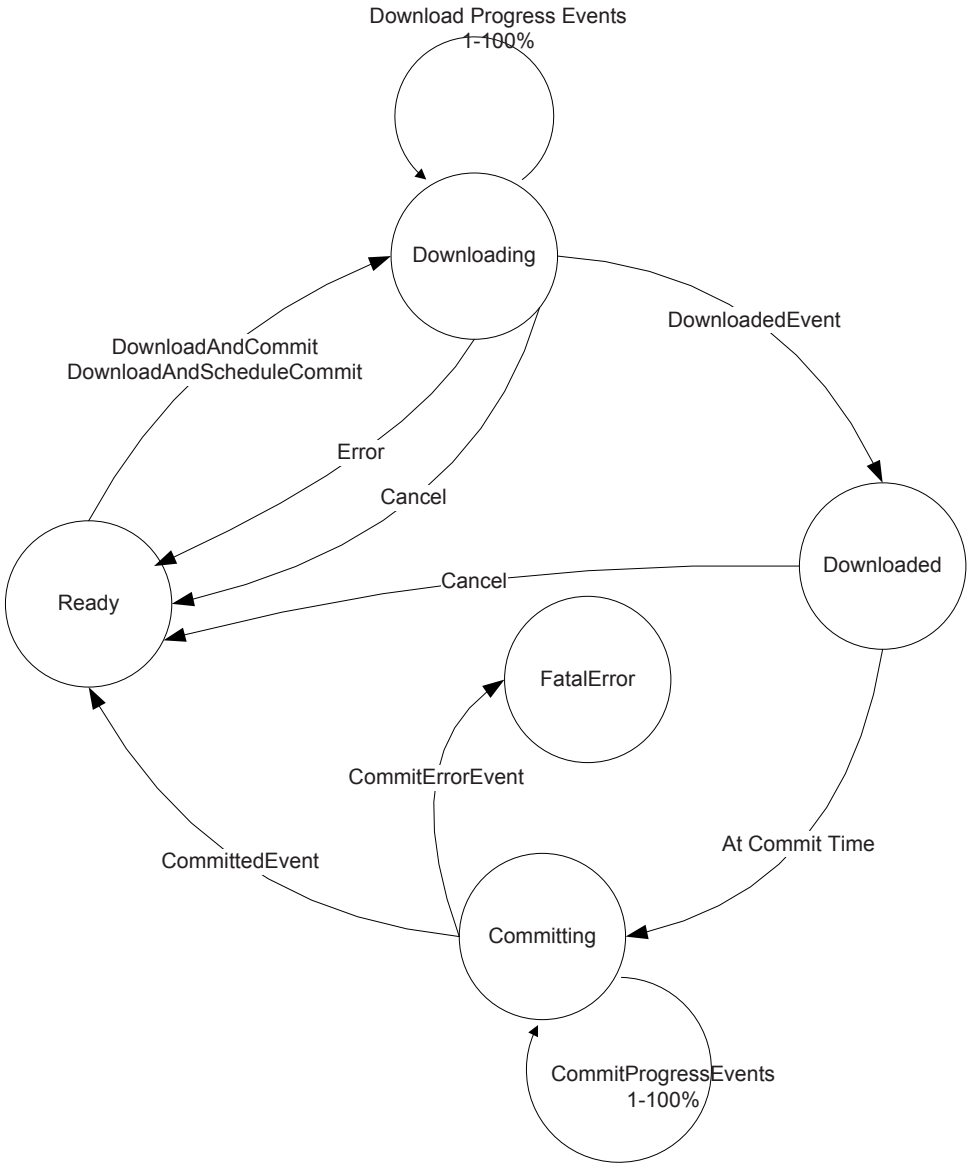


**Figure 3 — Service State Machine**

***Firmware States***

***Ready*** - The ready state is the initial state. The firmware service state is ready if the service is not downloading or committing firmware currently.

***Downloading*** – The service is currently downloading firmware to the device.

***Downloaded***: Firmware was successfully downloaded to the device. The firmware may be immediately committed or scheduled for a commit based on the client request.

***Committing*** - Firmware is currently being applied to the target.

***Fatal Error*** - There was an error during commit of firmware and the RF module is now unusable.

### 10.5.3 FUS Operations


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

#### 10.5.3.1 OperationNotPermittedInCurrentState

Any of the operations defined in FUS may return the **OperationNotPermittedInCurrentState** fault. This fault is sent when the FUS is not in one of the allowed states for this operation.

Table 2 lists the details for an operation fail in current state.

| Field | Value |
|---|---|
| [Code] | soap:Receiver |
| [Subcode] | rdmp:OperationNotPermittedInCurrentState |
| [Reason] | The service is not in one of the allowed states for this operation. |
| [Detail] | *Current state of the service. Allowed states for this operation.* |

**Table 2 — Fault Details for Operation Fail**

##### 10.5.3.1.1 DownloadandCommit

##### 10.5.3.1.2 General

This method shall be supported by the FUS.

If this operation is invoked in a state other than Ready, the FUS shall return OperationNotPermittedinCurrentState error. Once the FUS responds successfully to this operation, it shall move into the Downloading state.

NOTE It is best practice to invoke CheckFirmwareApplicability before invoking DownloadandCommit method

##### 10.5.3.1.3 Request Elements [Method Parameters for DownloadandCommit]

##### 10.5.3.1.4 FirmwareLocation

The URL from where the firmware is available for download.

The FUS shall support downloading firmware using HTTP. The FUS may support downloading firmware using HTTPS.

If the URL has an unsupported scheme, the FUS shall return an UnsupportedFirmwareLocationScheme fault. If the URL is invalid for other reasons, the FUS may return the InvalidRequestElement fault. The [Reason] element may have additional text to explain why the URL is invalid. Table 3 lists the details for the Firnware location.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

| Field | Value |
|---|---|
| [Code] | soap:Sender |
| [Subcode] | rdmp:UnsupportedFirmwareLocationScheme |
| [Reason] | The supplied FirmwareLocation has an unsupported URI scheme. |
| [Detail] | *<SupportedUriSchemes>*<br>*<!-- One or more supported URL schemes-->*<br>*<SupportedUriScheme>HTTP</SupportedUriScheme>*<br>*<SupportedUriScheme>HTTPS</SupportedUriScheme>*<br>*...*<br>*</SupportedUriSchemes>* |

**Table 3 — Details for FirmwareLocation**

Faults defined in this method may be generated by the FUS just by examining the FirmwareLocation URL syntactically. FUS provides another mechanism to address other errors such as the FirmwareLocation being unreachable. Since the firmware download is attempted in the Downloading state, if download fails, the FUS shall move into the Ready state. The error may be recorded by the FUS and reported in a GetStatus operation.

NOTE 1 The device may use HTTP Range headers to control the rate at which the download happens. The heuristics used to determine the size of the range and timing of (partial) HTTP(S) GET requests is left to the device.

NOTE 2 In case of error prone connections, range headers may be used to resume a download. It is the device's responsibility to determine the resume location in the firmware update file.

When the FUS does a partial HTTP GET, it shall use “bytes" as the Range Unit.

NOTE 3 As best practice, this standard recommends the following:- The HTTP server that serves firmware download requests should support partial HTTP GET using the Range header. It should support “bytes” as a Range Unit. It is the responsibility of the HTTP Server serving the firmware download request to specify and implement any policies with respect to the valid duration of the URL.

#### 10.5.3.2 Post Download

Once download is completed successfully, the FUS may raise a DownloadedEvent.

Once download is completed successfully, the FUS shall move into the Downloaded state.


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

The FUS is recommended to validate the firmware binary prior to committing. The mechanism used for validation is out of scope for this document. If the binary is found to be invalid, the FUS may record the error and report this in a GetStatus operation.

The FUS is expected to commit the firmware immediately once the download is complete.

NOTE The HTTP Server for FUS may be implemented in the same host as the RDMP client or hosted on a remote server.

#### 10.5.3.3 DownloadAndScheduleCommit

##### 10.5.3.3.1 General

This method may be supported by the FUS.

If this operation is invoked in a state other than Ready, the FUS shall return OperationNotPermittedinCurrentState error. Once the FUS responds successfully to this operation, it shall move into the Downloading state.

##### 10.5.3.3.2 Request Elements [Input Parameters]

###### 10.5.3.3.2.1 FirmwareLocation

Please see the DownloadandCommit section for description of requirements.

###### 10.5.3.3.2.2 AtTime

This is the date & time at which to commit the loaded firmware. If the AtTime is in the past, the FUS shall return an InvalidRequestElement error. Additional text may be added to the [Reason] element of the SOAP fault.

###### 10.5.3.3.2.3 PostDownload

Once download is completed successfully, the FUS may raise a DownloadedEvent.

Once download is completed successfully, the FUS shall move into the Downloaded state.

The FUS is recommended to validate the firmware binary prior to committing. The mechanism used for validation is out of scope for this document. If the binary is found to be invalid, the FUS may record the error and report this in a GetStatus operation.

#### 10.5.3.4 CheckFirmwareApplicability

##### 10.5.3.4.1 General

This method requests the device firmware update service to checks if specified firmware is applicable for the device. This method shall be supported by the FUS.

##### 10.5.3.4.2 Request Elements [Method Parameters]

###### 10.5.3.4.2.1 FirmwareVersionToCompare

The FirmwareVersion is the version of the firmware that the client wishes to compare with the committed firmware version on the FUS.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

This part of ISO/IEC 24791 does not mandate any specific requirements for the FirmwareVersion string. Implementations are recommended to construct a string that enables the device to determine

a) If the firmware being supplied is applicable to the FUS

b) If the firmware being supplied is newer or older

#### 10.5.3.4.3 Response Elements

The method returns one of the following

**Newer** – firmware is applicable to FUS and is more recent than the currently installed version

**Older** - firmware is applicable to FUS and is less recent than the currently installed version

**SameVersion** - firmware is applicable to FUS and is the same version as the currently installed version

**NotApplicable** - firmware is not applicable for the device or the supplied string is invalid or the FUS is unable to parse the string

### 10.5.3.5 GetStatus

#### 10.5.3.5.1 General

This method returns current state of firmware update service on the device.This method shall be supported by the FUS.

#### 10.5.3.5.2 Response Elements

The response shall contain the following field

**State** – one of Ready, Downloading, Downloaded, Committing, or FatalError

The response may contain the following fields:-

1. % downloaded - If state is Downloading, the FUS may return the % of firmware downloaded.
2. % committed - If state is committing, the FUS may return the % committed.
3. Error: The FUS may persist an error string from a previous operation or error situation.
4. TimeofError: the time at which the last error occurred.
5. Description – A localizable string. It applies to any state.

NOTE Let us say that while committing firmware there is an error and the service goes into the Ready state. The error may be stored in the service to be retrieved later by the client. The error string may also be used to diagnose errors encountered by the FUS.

### 10.5.3.6 Cancel

#### 10.5.3.6.1 General

This method may be supported by the FUS.


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

#### 10.5.3.6.2 Cancel Description

If this operation is invoked in the Ready state, it may be ignored. If the FUS is in the Downloading or Downloaded states, it shall move to the Ready state. In the Committing state, the FUS may reject the Cancel operation by returning the CancelNotPermittedNow error. Table 4 lists the details of the cancel method.

| Field | Value |
|---|---|
| [Code] | soap:Receiver |
| [Subcode] | rdmp: CancelNotPermittedNow |
| [Reason] | Cancel operation not permitted at this point. |
| [Detail] | None |

**Table 4 — Details of Cancel Method**

### 10.5.3.7 Events from FUS

#### 10.5.3.7.1 General

The FUS shall implement eventing as defined in the DPWS requirements for eventing. Please see section titled **Eventing** in the DPWS specification.

#### 10.5.3.7.2 DownloadProgressEvent

##### 10.5.3.7.2.1 General

DownloadProgressEvents may be generated only in the Downloading state.

##### 10.5.3.7.2.2 PercentCompleted

Percentage of download completed may be provided with the DownloadProgressEvent by the service. If provided, this shall be an integer between 0 and 100.

#### 10.5.3.7.3 DownloadedEvent

DownloadedEvent may be generated when the service transitions from the Downloading state to the Downloaded state.

#### 10.5.3.7.4 CommitProgressEvent

##### 10.5.3.7.4.1 General

CommitProgressEvents may be generated only in the Committing state.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

#### 10.5.3.7.4.2 PercentCompleted

Percentage of update completed may be provided with the CommitProgressEvent by the service. If provided, this shall be an integer between 0 and 100

#### 10.5.3.7.4.3 Description

This is a descriptive localizable string about the status of the commit.

#### 10.5.3.7.5 CommittedEvent

CommittedEvent may be generated when the service transitions from the Committing state to the Ready state.

#### 10.5.3.7.6 CommitErrorEvent

#### 10.5.3.7.6.1 General

If there is an error during firmware commit, it may be reported using the CommitErrorEvent.

#### 10.5.3.7.6.2 Description

This is a localizable string containing a description of what went wrong during the firmware commit.

#### 10.5.3.7.6.3 Time

This is the time at which this particular error took place.

#### 10.5.3.7.7 DownloadErrorEvent

If there is an error during firmware download, it may be reported using the DownloadErrorEvent.

## 10.6 Management Service (MS)

### 10.6.1 General

This section describes a Management Service (MS). The management service provides the following functionality:-

a. Configuring a device with standard properties. In this document, we include the ability to configure ISO/IEC 24791-5 properties on the device.

b. Implementing common operations like device reboot and reset to factory settings.

The MS specifies a set of configuration properties that are commonly understood among RFID device implementations. The MS also allows for custom configuration properties to be retrieved and applied on devices. The MS also provides a mechanism to advertise metadata for configuration properties.

Each configuration property has a unique identifier and a value associated with the identifier.

### 10.6.2 Property Identifier

A property identifier has two parts:-

1. **Group URI** - (example: http://standards.iso.org/24791-3/rdmp/Configuration/RF). The Group URI acts as a namespace.


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

2. **Property Name** - (example: "Power Level")

A Property Name shall be of type token as defined in XML Schema Part 2.

*Token: token represents tokenized strings. The value space of token is the set of strings that do not contain the carriage return (#xD), line feed (#xA) nor tab (#x9) characters, that have no leading or trailing spaces (#x20) and that have no internal sequences of two or more spaces. The lexical space of token is the set of strings that do not contain the carriage return (#xD), line feed (#xA) nor tab (#x9) characters, that have no leading or trailing spaces (#x20) and that have no internal sequences of two or more spaces.*

A property identifier used by MS shall NOT have null value for either the group URI or the Property Name

### 10.6.3 Property Value Metadata

Metadata of the property value is made up of the following:-

- **Description** – Friendly description of the property. It is of type string. A MS service shall include description in the metadata.
- **Writeable** – A property is writeable if it may be modified on the device. It is of type Boolean. MS may include this field in the metadata. If this is not specified, the client may assume the property to be writeable.
- **Persisted** – A property is persisted if the device stores the property in permanent storage. . It is specified as a Boolean. MS may include this in the metadata. If this is not specified, the client may assume the property to be persisted.
- **RestartRequired** - Does device requires a restart for the change in the property to take effect – This is specified as a Boolean. MS may include this in the metadata. If this is not specified, the client may assume that restart is not required.
- **Type** – the type of the property, indicating if the property is of the type string, int, boolean, or some other complex type. The MS shall include the type in the metadata. The type shall be a XML QName, as defined in the XML Schema as defined in XML Schema Part 2: Datatypes.
- **DefaultValue** – The value that the device uses if the client has not modified. It may be included. If included, it shall conform to the Type specified in the metadata.

NOTE The type metadata is critical for clients to interpret and process configuration data sent by the device.

### 10.6.4 Device Property Profile

A property profile is a collection of properties.

NOTE Using a collection of properties is useful in many scenarios. Management software may want to bring the device to a base configuration, when it is first discovered. When a device changes role, role specific configuration may need to be applied to the device. Using a property profile enables device and clients to store a collection of properties together.

### 10.6.5 Sources and Source Types

Sources in RDMP may refer to the device or the antennas or physical ports connected to the device. The standard source types are antenna, GPI, GPO and Barcode.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014

### 10.6.6 MS Operations

#### 10.6.6.1 GetSources

##### 10.6.6.1.1 General

This method is invoked by the client to get the list of sources on the device and the types of the sources. This method shall be supported by MS.

##### 10.6.6.1.2 Request Elements

None

##### 10.6.6.1.3 Response Elements

This method returns a collection of the following tuples. Each tuple shall have

**SourceName** – of type token, as defined in XML Schema

**Type** – Source Type

#### 10.6.6.2 GetAllPropertyMetadata

##### 10.6.6.2.1 General

This method shall be supported by MS. This is the mechanism for a client to obtain a list of supported properties and property metadata.

NOTE GetAllPropertyMetadata is the key method for a client to discover device and source related configuration. It is recommended that the Management Service provide comprehensive metadata information about all the properties configurable via RDMP. Metadata enables the management software to correctly display configuration (example: a property may be shown disabled in the user interface if it is not writeable). It also enables management software to warn the user to reboot the device if the property change requires a restart to take effect.

##### 10.6.6.2.2 Request Elements

**SourceName** – this is of type string. This field is optional.

If the SourceName parameter is not specified, this method shall return the metadata associated with all the properties of the device.

If the SourceName parameter is specified, this method shall return the metadata associated with all the properties of the specified source.

##### 10.6.6.2.3 Response Elements

The method returns a collection of property identifiers and property value metadata.

#### 10.6.6.3 GetPropertyMetadata

##### 10.6.6.3.1 General

This method may be supported by MS.


© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24791-3:2014