INTERNATIONAL STANDARD

ISO/IEC 24791-3

Second edition
2022-12

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 24791-3:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/IEC 24791-3:2014), which has been technically revised.

The main changes compared to the previous edition are: the references have been updated to the latest standards.

A list of all parts in the ISO ISO/IEC 24791 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Radio frequency identification (RFID) air interface technology is based on non-contact electromagnetic 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 have to provide secure and interoperable services, interfaces, and technologies. This is the goal of the ISO/IEC 24791 series, created for RFID software system infrastructure (SSI).

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

Part 3: Device management

1 Scope

1.1 General

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

This document provides two distinct *interface sets*, one based on the GS1 EPCglobal DCI standard and the IETF SNMP RFCs and the other based on the Organization for the Advancement of Structured Information Standards (OASIS) DPWS standard. The definition of the Device Profile for RFID is referred to in this document 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:

- the 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 document allow for clients and services endpoints to implement and provide the services based on the specific characteristics of the RFID system to be implemented. Subclause 1.2 defines the Conformance requirements for systems that implement components of one or both of the interface sets.

1.2 Conformance

This document 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 document.

1.3 DCI and SNMP interface set

This document divides the DCI capabilities into two *Conformance Groups:*

- Discovery, Configuration, and Initialization Conformance Group: this Conformance Group is defined in Clause 7. It specifies the protocols and operational procedures that are required for conforming Interrogator Implementations and Device Management Implementations, as defined in this document as well as in ISO/IEC 24791-1.

- Performance Monitoring and Diagnostics Conformance Group: this Conformance Group is defined in Clause 8. It specifies the SNMP MIBs that can be implemented by Interrogator Implementations and Data Management Implementations as defined in this document 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 has to 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.

1.4 RDMP interface set

This document 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.

RDMP interface set is defined in Clause 9.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

Devices Profile for Web Services (DPWS) 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.

GS1 Discovery, Configuration, & Initialisation (DCI) Standard for Reader Operations, https://www.gs1.org/standards/epc-rfid

GS1 Reader Management, (RM v1.0.1), Ratified Standard, https://www.gs1.org/standards/epc-rfid

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
component
identifiable part of a service that provides specific functionality

3.2
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

3.3
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

3.4
endpoint
component (3.1) that implements or exposes an interface to other components or uses the interface of another component

3.5
implementation
software and hardware that provides the reduction to practice of particular functionality

3.6
interrogator controller
software capability possibly embodied in a distinct physical device, within the *data management* (3.2) *implementation* (3.5) 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

3.7
client
network *endpoint* (3.4) that sends messages to and/or receives messages from a service

3.8
hosted service
service with lifecycle under the control of another service

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 19762 and the following shall apply.

AC	Access controller
CAPWAP	Control and provisioning of wireless access pints
DCI	Discovery, configuration, initialization
DPWS	Devices profile for web services standard
IETF	Internet engineering task force
LLRP	Low level reader protocol
MIB	Management information base
MIB-II	Management information base version 2
RDMP	RFID device management profile
RFC	Request for comment
RM	Reader management
SNMP	Simple network management protocol
SOAP	Simple object access protocol
SSI	Software system infrastructure

UML	Unified modelling language
URI	Uniform resource identifier
URL	Uniform resource locator
WTP	Wireless termination point
FUS	RDMP firmware update service
MS	Management service
MNS	Monitoring service

5 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.

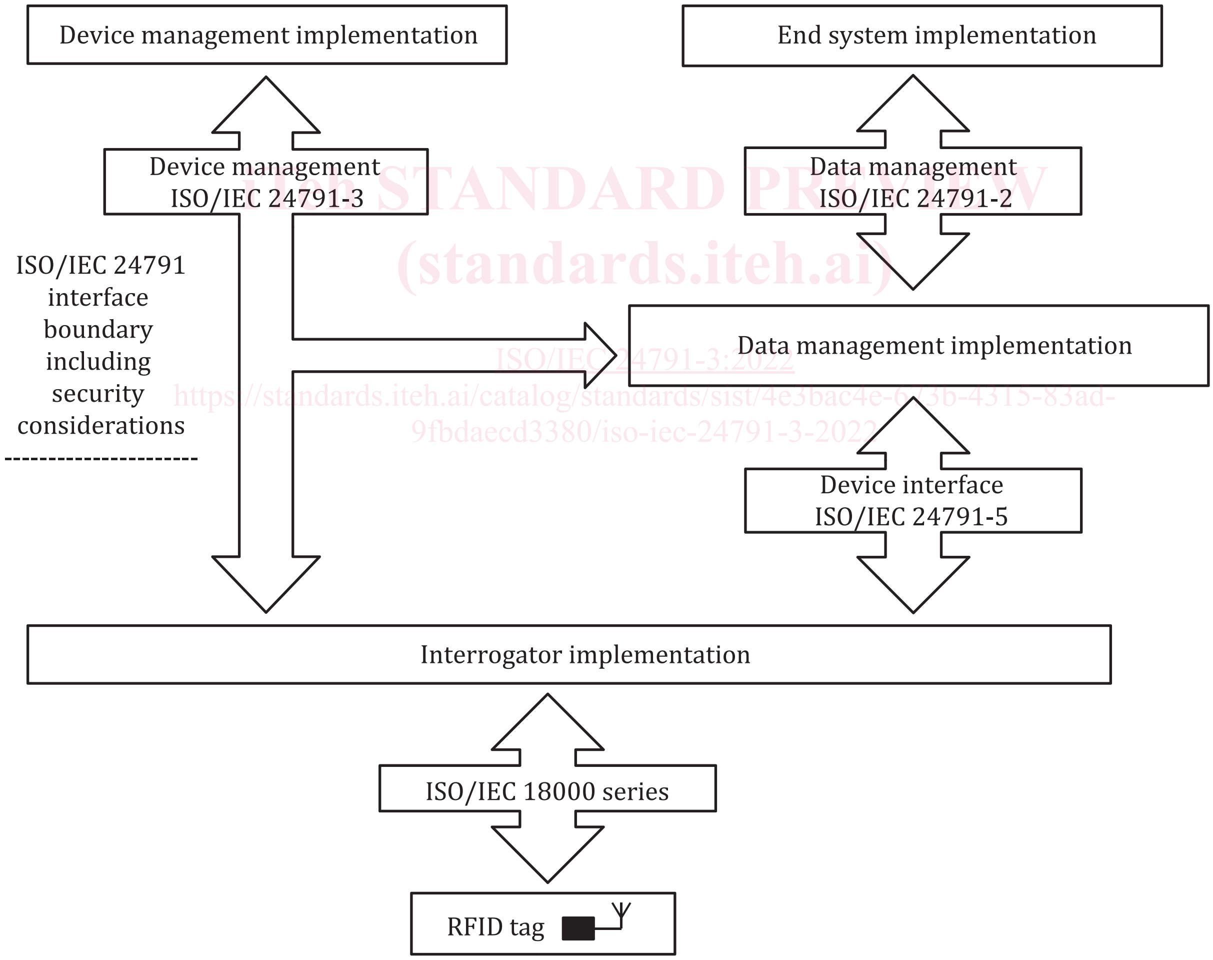

Figure 1 — Architecture overview including relationships to other RFID standards

The parts of the ISO/IEC 24791 series that define Data Management (i.e. ISO/IEC 24791-2), Device Interface (i.e. ISO/IEC 24791-5), and Device Management (i.e. this document) 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 24791-1, 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 series that is important. Examples of different deployment models of this document are provided in Annex A.

6 UML modelling

Although Figure 1 provides a general overview of the relationship between the interfaces and implementations in the SSI, 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 can exist in standards compliant solutions, respectively. Refer to ISO/IEC 24791-1 for a more complete description of how UML is used in other parts of the ISO/IEC 24791 series.

7 Device management

7.1 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.

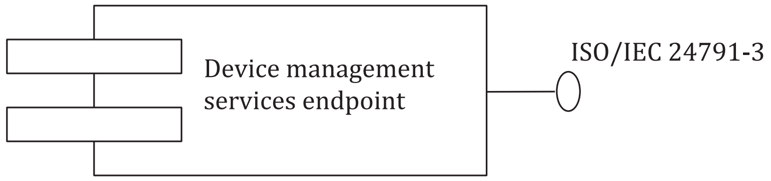

Figure 2 — Device management representation

The software programs that provide device management client and services endpoints can reside within any of the Implementations that can exist in the SSI, as shown in Figure 1. This document does define requirements on 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 ISO/IEC 24791-5 and ISO/IEC 24791-2, respectively. 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 can 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 document or in ISO/IEC 24791-1.

The functions covered by device management can 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 can be defined for other SSI software components, but diagnostic capabilities for general purpose computing platforms will not be defined.

The interfaces defined by this document will provide extension mechanisms to allow implementations to expose management services beyond those specifically defined in this document. 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 6.

8 DCI and SNMP interface set

8.1 Discovery, configuration and initialization conformance group

8.1.1 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 document references the GS1 EPCglobal DCI for reader operations standard for the normative requirements for this SSI capability. The GS1 EPCglobal DCI standard, references the IETF CAPWAP standard for the core network protocol, security, and communication operations and interfaces.

8.1.2 Interrogator implementations

Interrogators that conform to this document for discovery, configuration and initialization capabilities shall implement all requirements, indicated with “shall”, for the *Reader* function as defined in the GS1 EPCglobal DCI standard. Conforming implementations may implement any requirements for the Reader function indicated with “may” in the GS1 EPCglobal DCI standard.

8.1.3 Device management implementations

Device management implementations that conform to this document shall implement all requirements, indicated with “shall” for the AC function as specified in the GS1 EPCglobal DCI standard. Conforming implementations may implement any requirements indicated with “may” in the GS1 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.

8.2 Performance monitoring and diagnostics conformance group

8.2.1 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. SNMP clients (client endpoints in the SSI architecture) access the exposed device management information using the 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 document 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.

8.2.2 Interrogator implementations

The GS1 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 GS1 EPCglobal Reader Management Version 1.0.1 specification shall be implemented by interrogators that claim conformance to this subclause.

Implementation of non-SNMP bindings or transports described in the GS1 EPCglobal Reader Management standard is not required by this document.

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

a) the MIB-II System Group, defined in the SNMPv2-MIB module in RFC 3418;

b) the MIB-II IP Group, defined in the IP-MIB module in RFC 2011;

c) the MIB-II Interfaces Group, defined in the IF-MIB in RFC 2863.

8.2.3 Data management implementations providing interrogator controller functionality

Annex B provides an SNMP MIB for performance monitoring and diagnostic information access of data management implementations that implement a device interface (see 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 shall be implemented by interrogator controller functions within data management implementations that claim conformance to this subclause. 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 MIB in Annex B in a future version of this document.

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

a) the MIB-II System Group, defined in the SNMPv2-MIB module in RFC 3418;

b) the MIB-II IP Group, defined in the IP-MIB module in RFC 2011;

c) the MIB-II Interfaces Group, defined in the IF-MIB in RFC 2863.

9 RDMP interface set

9.1 General

The following subclauses define the RDMP interface set.

A conforming RDMP implementation shall implement DEVICE as defined in DPWS

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

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

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

9.2 XML namespace

In addition to the namespaces defined in DPWS, this document defines the following XML namespace:

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

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

Table 1 — XML namespaces

Prefix	XML namespace	Specification
Rdmp	https://standards.iso.org/iso-iec/24791/-3/ed-2/en/rdmp/	ISO/IEC 24791-3
Dpws	http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01	DPWS
Soap	http://www.w3.org/2003/05/soap-envelope	DPWS
Was	http://www.w3.org/2005/08/addressing	DPWS

9.3 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 Hello and Probe Match messages.

A conformant RDMP device will have dpws:device and rdmp:ISO24791-3 in the Types section of discovery Hello and Probe Match message.

A transport address may be sent by an RDMP device in the Hello and Probe Match messages defined in WS-Discovery.

NOTE DPWS uses WS-Discovery as the device discovery protocol. WS-Discovery defines a multicast discovery protocol. Clients discovering RDMP devices joins the multicast group defined in WS-Discovery and discovers RDMP devices on the network from Hello multicast message or a Probe Match unicast response message in response to a Probe multicast message from the client, where the RDMP devices advertises dpws: device and rdmp:ISO24791-3 in the Types section of the Hello or Probe Match message.

9.4 Device metadata

9.4.1 General

This document 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 includes information such as manufacturer name, model name, firmware version, etc. This mechanism is documented in the Description Section in the DPWS spec. This document describes it briefly for illustration in 9.4.2 EXAMPLES 1 and 2.

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 then sends a WS-Transfer GetResponse message containing the device metadata.

NOTE 3 Refer to Devices Profile for Web Services Version 1.1 section titled "Description" for more details and requirements.

9.4.2 Service discovery

An RDMP conformant device may advertise services that are not specified in this document 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.

EXAMPLE 1 An example response that advertises a printer service is:

```
<?xml version="1.0" encoding="utf-8"?>
<wsoap12:Envelope
    xmlns:wsoap12="http://www.w3.org/2003/05/soap-envelope"
```