INTERNATIONAL STANDARD

ISO/IEC 17811-1

First edition
2014-06-15

Information technology — Device control and management —

Part 1: Architecture

Technologies de l'information — Commande et gestion de périphériques —
Partie 1: Architecture

Reference number
ISO/IEC 17811-1:2014(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

Page

Foreword

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

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 document 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 and IEC 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 31, *Automatic identification and data capture techniques*.

ISO/IEC 17811 consists of the following parts, under the general title *Information technology — Device control and management*:

— *Part 1: Architecture*

— *Part 2: Specification of Device Control and Management Protocol*

— *Part 3: Specification of Reliable Message Delivery Protocol*

Introduction

This International Standard provides the architecture for device control and management (DCM). DCM can support the various control and management services, regardless of the network protocols or interfaces. DCM is composed of two protocols: DCMP (Device Control and Management Protocol) and RMDP (Reliable Message Delivery Protocol).

This International Standard consists of the following parts:

— Part 1: Architecture

— Part 2: Specification of Device Control and Management Protocol (DCMP)

— Part 3: Specification of Reliable Message Delivery Protocol (RMDP)

Part 1 of ISO/IEC 17811 describes the architecture of DCM, which includes definition, general concept, requirements, design principles, service scenarios for device management control, and management.

Part 2 of ISO/IEC 17811 specifies the Device Control and Management Protocol (DCMP), which includes the functional entities, protocol operations, message structure, and detailed parameter format associated with DCMP.

Part 3 of ISO/IEC 17811 specifies the Reliable Message Delivery Protocol (RMDP), which includes the interworking with DCMP, protocol operations, and message structure associated with RMDP.

Information technology — Device control and management —

Part 1: Architecture

1 Scope

This International Standard provides the relationship between DCMP and RMDP with use cases. Also, this International Standard specifies the requirements and design principles.

2 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 17811-2, *Information technology — Device control and management — Part 2: Specification of Device Control and Management Protocol*

ISO/IEC 17811-3, *Information technology — Device control and management — Part 3: Specification of Reliable Message Delivery Protocol*

3 Terms and definitions

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

3.1
device control and management
DCM
operations are purposed to control and manage the various smart devices. For this purpose, DCM is composed of two protocols; DCMP (Device Control and Management Protocol) and RMDP (Reliable Message Delivery Protocol)

3.2
device control and management protocol
DCMP
used to perform various management operations which are categorized into information retrieval, control, diagnostic, and debugging

3.3
reliable message delivery protocol
RMDP
used to provide uniform and reliable message delivery among devices regardless of the underlying network protocols or interfaces

3.4
administrative domain
represents a network area where a single administrator can configure and manage a network with the same policy

3.5
device management server
DMS
used to keep track of the various device information and also to manage the devices in an administrative domain

Note 1 to entry: There can be one DMS in an administrative domain, if needed.

3.6
DCM device
represents a device that supports the RMDP and DCMP message exchange, parsing, and processing

3.7
node information
information which is managed by RMDP, such as physical address identifier, device identifier, and so on

4 Abbreviations

The following acronyms are used in this International Standard.

DCM device control and management

DCMP device control and management protocol

DHCP dynamic host configuration protocol

DMS device management server

RMDP reliable message delivery protocol

UUID universally unique identifier

UPnP universal plug and play

5 Overview

DCM provides various functions for the device management. DCM supports the device and network status information retrieval, device and network initialization, firmware and software update, file transmission and so on. In an administrative domain, there may be a device management server that collects, controls, and manages devices using DCMP. To exchange DCMP messages among the devices, RMDP is needed. RMDP is a message exchange protocol among the devices regardless of the network protocols or interfaces. The detailed protocol stack of DCM is illustrated in the Figure 1.

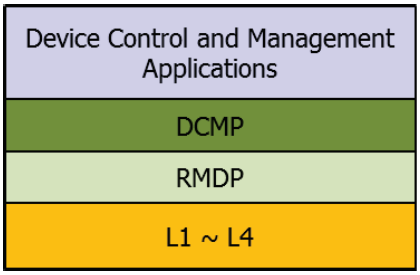

Figure 1 — Protocol Stack for the DCM

Basically, DCMP messages can be exchanged using the RMDP. RMDP has node information, which maintains the mapping information between DCM device identifier and physical network identifier, such as the IP address and port number in IP network. If there is a device management server (DMS) in an administrative domain, the RMDP might be able to obtain the node information about all devices that

are connected in the administrative domain from the DMS. Note : There are several ways to retrieve node information. For example, the RMDP is able to request node information by using the RMDP messages when there is no DMS or when DMS does not response. Therefore the node retrieval mechanisms depend on implementation. When the RMDP retrieves the node information without DMS, the integrity of node information may not be guaranteed

After RMDP retrieves the target node information, DCMP messages, such as 'DEVICE_INFORMATION_REQUEST' or 'DEVICE_CONTROL_REQUEST', can be transferred to the target device using RMDP.

6 DCM Service Environments

6.1 Case 1: Local Network with Device Management Server

Figure 2 shows an example of DCM service environment where all devices and a management server are connected in a local network with device management server (DMS). The DMS retrieves device information in the administrative domain and manages devices with DCMP. In this environment the information device, such as smart phone, is able to control the devices using the DCMP. When smart phone join the administrative domain, RMDP on smart phone could find the DMS and receive the node information about whole devices which are connected in that administrative domain from the DMS. Then DCMP on the smart phone sends the device discovery request message to the other devices and receives the response message by using the RMDP. After that, smart phone is able to see the all devices in the network. If the target device is selected and control information is available by user, DCMP generates and transmits the device control request messages to the target device by using the RMDP.

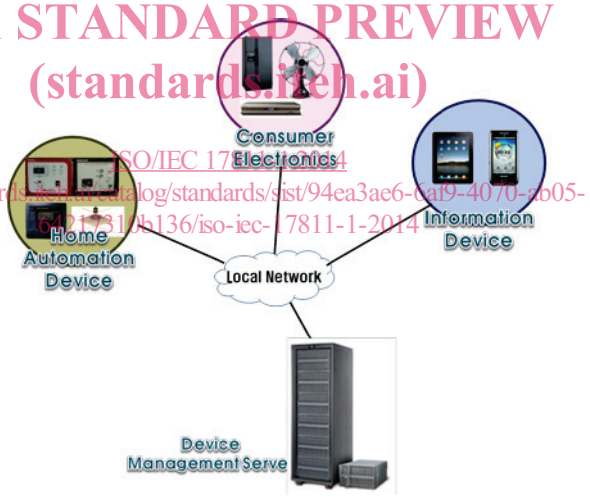

Figure 2 — DCM service environment case 1: Local network with device management server

6.2 Case 2: Local Network without Device Management Server

Figure 3 shows the example of DCM service environment where all devices are connected in the local network without device management server. The information device, such as smart phone, can control the DCM devices by using the DCM based application. When a node discovery request message is broadcasted by RMDP on the smart phone, RMDPs on the other devices which receive the node discovery request message would response with their node information. Then DCMP on the smart phone sends the device discovery request message to the other devices and receives the response message by using the RMDP. After that, smart phone is able to see the all devices in the network. If the target device is selected and control information is entered by user, DCMP generates the device control request message and sends that control message to the target device by using the RMDP.