INTERNATIONAL STANDARD

ISO/IEC 29341-12-2

Second edition
2015-06-15

Information technology — UPnP Device Architecture —

Part 12-2: Remote User Interface Device Control Protocol — Remote User Interface Server Device

Technologies de l'information — Architecture de dispositif UPnP —

Partie 12-2: Protocole de contrôle de dispositif d'interface utilisateur à distance — Dispositif serveur d'interface utilisateur à distance

Reference number
ISO/IEC 29341-12-2:2015(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

LIST OF TABLES

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 http://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 the 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

ISO/IEC 29341-12-2 was prepared by UPnP Implementers Corporation and adopted, under the PAS procedure, by joint technical committee ISO/IEC JTC 1. Information technology, in parallel with its approval by national bodies of ISO and IEC.

This second edition replaces the first edition (ISO/IEC 29341-12-2:2008), which has been technically revised.

The list of all currently available parts of ISO/IEC 29341 series, under the general title *Information technology — UPnP Device Architecture*, can be found on the ISO web site.

Introduction

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the use of patents as indicated below.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights. The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Intel Corporation has informed ISO and IEC that it has patent applications or granted patents.

Information may be obtained from:

Intel Corporation
Standards Licensing Department
5200 NE Elam Young Parkway
MS: JFS-98
USA – Hillsboro, Oregon 97124

Microsoft Corporation has informed ISO and IEC that it has patent applications or granted patents as listed below:

6101499 / US; 6687755 / US; 6910068 / US; 7130895 / US; 6725281 / US; 7089307 / US; 7069312 / US; 10/783 524 /US

Information may be obtained from:

Microsoft Corporation
One Microsoft Way
USA – Redmond WA 98052

Philips International B.V. has informed ISO and IEC that it has patent applications or granted patents.

Information may be obtained from:

Philips International B.V. – IP&S
High Tech campus, building 44 3A21
NL – 5656 Eindhoven

NXP B.V. (NL) has informed ISO and IEC that it has patent applications or granted patents.

Information may be obtained from:

NXP B.V. (NL)
High Tech campus 60
NL – 5656 AG Eindhoven

Matsushita Electric Industrial Co. Ltd. has informed ISO and IEC that it has patent applications or granted patents.

Information may be obtained from:

Matsushita Electric Industrial Co. Ltd.
1-3-7 Shiromi, Chuoh-ku
JP – Osaka 540-6139

Hewlett Packard Company has informed ISO and IEC that it has patent applications or granted patents as listed below:

5 956 487 / US; 6 170 007 / US; 6 139 177 / US; 6 529 936 / US; 6 470 339 / US; 6 571 388 / US; 6 205 466 / US

Information may be obtained from:

Hewlett Packard Company
1501 Page Mill Road
USA – Palo Alto, CA 94304

Samsung Electronics Co. Ltd. has informed ISO and IEC that it has patent applications or granted patents.

Information may be obtained from:

Digital Media Business, Samsung Electronics Co. Ltd.
416 Maetan-3 Dong, Yeongtang-Gu,
KR – Suwon City 443-742

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Original UPnP Documents

Reference may be made in this document to original UPnP documents. These references are retained in order to maintain consistency between the specifications as published by ISO/IEC and by UPnP Implementers Corporation. The following table indicates the original UPnP document titles and the corresponding part of ISO/IEC 29341:

UPnP Document Title	ISO/IEC 29341 Part
UPnP Device Architecture 1.0	ISO/IEC 29341-1
UPnP Basic:1 Device	ISO/IEC 29341-2
UPnP AV Architecture:1	ISO/IEC 29341-3-1
UPnP MediaRenderer:1 Device	ISO/IEC 29341-3-2
UPnP MediaServer:1 Device	ISO/IEC 29341-3-3
UPnP AVTransport:1 Service	ISO/IEC 29341-3-10
UPnP ConnectionManager:1 Service	ISO/IEC 29341-3-11
UPnP ContentDirectory:1 Service	ISO/IEC 29341-3-12
UPnP RenderingControl:1 Service	ISO/IEC 29341-3-13
UPnP MediaRenderer:2 Device	ISO/IEC 29341-4-2
UPnP MediaServer:2 Device	ISO/IEC 29341-4-3
UPnP AV Datastructure Template:1	ISO/IEC 29341-4-4
UPnP AVTransport:2 Service	ISO/IEC 29341-4-10
UPnP ConnectionManager:2 Service	ISO/IEC 29341-4-11
UPnP ContentDirectory:2 Service	ISO/IEC 29341-4-12
UPnP RenderingControl:2 Service	ISO/IEC 29341-4-13
UPnP ScheduledRecording:1	ISO/IEC 29341-4-14
UPnP DigitalSecurityCamera:1 Device	ISO/IEC 29341-5-1
UPnP DigitalSecurityCameraMotionImage:1 Service	ISO/IEC 29341-5-10
UPnP DigitalSecurityCameraSettings:1 Service	ISO/IEC 29341-5-11
UPnP DigitalSecurityCameraStillImage:1 Service	ISO/IEC 29341-5-12
UPnP HVAC_System:1 Device	ISO/IEC 29341-6-1
UPnP HVAC_ZoneThermostat:1 Device	ISO/IEC 29341-6-2
UPnP ControlValve:1 Service	ISO/IEC 29341-6-10
UPnP HVAC_FanOperatingMode:1 Service	ISO/IEC 29341-6-11
UPnP FanSpeed:1 Service	ISO/IEC 29341-6-12
UPnP HouseStatus:1 Service	ISO/IEC 29341-6-13
UPnP HVAC_SetpointSchedule:1 Service	ISO/IEC 29341-6-14
UPnP TemperatureSensor:1 Service	ISO/IEC 29341-6-15
UPnP TemperatureSetpoint:1 Service	ISO/IEC 29341-6-16
UPnP HVAC_UserOperatingMode:1 Service	ISO/IEC 29341-6-17
UPnP BinaryLight:1 Device	ISO/IEC 29341-7-1
UPnP DimmableLight:1 Device	ISO/IEC 29341-7-2
UPnP Dimming:1 Service	ISO/IEC 29341-7-10
UPnP SwitchPower:1 Service	ISO/IEC 29341-7-11
UPnP InternetGatewayDevice:1 Device	ISO/IEC 29341-8-1
UPnP LANDevice:1 Device	ISO/IEC 29341-8-2
UPnP WANDevice:1 Device	ISO/IEC 29341-8-3
UPnP WANConnectionDevice:1 Device	ISO/IEC 29341-8-4
UPnP WLANAccessPointDevice:1 Device	ISO/IEC 29341-8-5
UPnP LANHostConfigManagement:1 Service	ISO/IEC 29341-8-10
UPnP Layer3Forwarding:1 Service	ISO/IEC 29341-8-11
UPnP LinkAuthentication:1 Service	ISO/IEC 29341-8-12
UPnP RadiusClient:1 Service	ISO/IEC 29341-8-13
UPnP WANCableLinkConfig:1 Service	ISO/IEC 29341-8-14
UPnP WANCommonInterfaceConfig:1 Service	ISO/IEC 29341-8-15
UPnP WANDSLLinkConfig:1 Service	ISO/IEC 29341-8-16
UPnP WANEthernetLinkConfig:1 Service	ISO/IEC 29341-8-17
UPnP WANIPConnection:1 Service	ISO/IEC 29341-8-18
UPnP WANPOTSLinkConfig:1 Service	ISO/IEC 29341-8-19
UPnP WANPPPConnection:1 Service	ISO/IEC 29341-8-20
UPnP WLANConfiguration:1 Service	ISO/IEC 29341-8-21
UPnP Printer:1 Device	ISO/IEC 29341-9-1
UPnP Scanner:1.0 Device	ISO/IEC 29341-9-2
UPnP ExternalActivity:1 Service	ISO/IEC 29341-9-10
UPnP Feeder:1.0 Service	ISO/IEC 29341-9-11

UPnP Document Title	ISO/IEC 29341 Part
UPnP PrintBasic:1 Service	ISO/IEC 29341-9-12
UPnP Scan:1 Service	ISO/IEC 29341-9-13
UPnP QoS Architecture:1.0	ISO/IEC 29341-10-1
UPnP QosDevice:1 Service	ISO/IEC 29341-10-10
UPnP QosManager:1 Service	ISO/IEC 29341-10-11
UPnP QosPolicyHolder:1 Service	ISO/IEC 29341-10-12
UPnP QoS Architecture:2	ISO/IEC 29341-11-1
UPnP QOS v2 Schema Files	ISO/IEC 29341-11-2
UPnP QosDevice:2 Service	ISO/IEC 29341-11-10
UPnP QosManager:2 Service	ISO/IEC 29341-11-11
UPnP QosPolicyHolder:2 Service	ISO/IEC 29341-11-12
UPnP RemoteUIClientDevice:1 Device	ISO/IEC 29341-12-1
UPnP RemoteUIServerDevice:1 Device	ISO/IEC 29341-12-2
UPnP RemoteUIClient:1 Service	ISO/IEC 29341-12-10
UPnP RemoteUIServer:1 Service	ISO/IEC 29341-12-11
UPnP DeviceSecurity:1 Service	ISO/IEC 29341-13-10
UPnP SecurityConsole:1 Service	ISO/IEC 29341-13-11

INFORMATION TECHNOLOGY – UPNP DEVICE ARCHITECTURE –

Part 12-2: Remote User Interface Device Control Protocol – Remote User Interface Server Device

1. Scope

This device template is compliant with the UPnP Architecture, Version 1.0.

This document defines the device
urn:schemas-upnp-org:device:*RemoteUIServerDevice:1*.

This device can be a UPnP root device, or embedded within a different device.

The *RemoteUIServerDevice* encapsulates all services for the Remote UI Server Device Control Protocol (DCP).

2. Device Definitions

2.1. Device Type

The following device type identifies a device that is compliant with this template:

urn:schemas-upnp-org:device:*RemoteUIServerDevice:1*

2.2. Device Model

It is recommended that *RemoteUIServerDevice* be implemented with support for securing UPnP™ actions. It is also recommended that securing of UPnP™ action is done using the *DeviceSecurity* service as defined by the UPnP™ security working committee. If implemented, the *DeviceSecurity* service must be contained either inside *RemoteUIServerDevice* implementation or in a device that encompasses the *RemoteUIServerDevice*. These two models are described below.

2.2.1. Description of Device Requirements

The following table briefly describes the service used in *RemoteUIServerDevice*.

Table 1: *RemoteUIServerDevice* Service Descriptions

Service Name	Service Description
RemoteUIServer	Allows for basic discovery of available and remotable user interfaces.
DeviceSecurity	Actions for taking ownership, configuring access control, establishing secure sessions, and invoking secure actions.

2.2.1.1. DeviceSecurity within RemoteUIServerDevice

This model is typically applicable to physical devices that need *DeviceSecurity* functionality (including device ownership and access control) to be used only by the *RemoteUIServerDevice*. In this case, products that expose devices of the type **urn:schemas-upnp-org:device:***RemoteUIServerDevice:1* must implement minimum version numbers of the required service specified in the table below.

Table 2: Device Requirements for stand-alone *RemoteUIServerDevice*

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
RemoteUIServerDevice:1	*Yes*	*R*	*RemoteUIServer:1*	*R*	*RemoteUIServer*
			DeviceSecuirty:1	*O*	*DeviceSecurity*
			Non-standard services embedded by an UPnP vendor go here.	*X*	*To be defined by vendor*

[1] R = Required, O = Optional, X = Non-standard.
[2] Prefixed by **urn:upnp-org**:**serviceId**:

Relationship between Services

Figure 1 shows the logical structure of the device and services defined by the working group for UPnP™ technology enabled Remote UI servers.

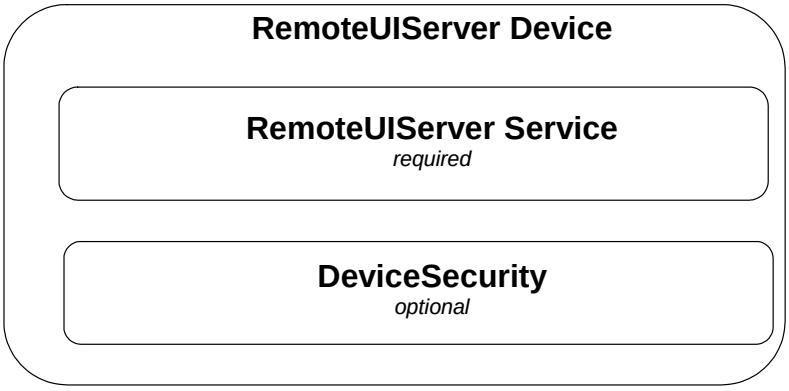

Figure 1: *DeviceSecurity* within *RemoteUIServerDevice*

2.2.1.2. DeviceSecurity outside RemoteUIServerDevice

This model is typically applicable to physical devices that implement Remote UI server functionality, but the *RemoteUIServerDevice* may use *DeviceSecurity* that is already part of another device. An example of this would be where **urn:schemas-upnp-org:device:** *RemoteUIServerDevice:1* is implemented inside a device of the type **urn:schemas-upnp-org:device:** *BasicDevice:1*. The *BasicDevice* in this case contains the *DeviceSecurity* service that may be used by another UPnP™ device e.g., *MediaRenderer*. The implementation of *RemoteUIServerDevice* must contain the minimum version number of the service specified in the table below.

Table 3: Device Requirements for embedded *RemoteUIServerDevice*

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
RemoteUIServerDevice:1	*Yes*	*R*	*RemoteUIServer:1*	*R*	*RemoteUIServer*
			Non-standard services embedded by an UPnP vendor go here.	*X*	*To be defined by vendor*

[1] R = Required, O = Optional, X = Non-standard.
[2] Prefixed by urn:**upnp-org**:**serviceId**: .

Relationships between Services

Figure 2 shows the logical structure of the device and services defined by the working group for UPnP™ technology enabled Remote UI servers that may use the *DeviceSecurity* service for other UPnP™ devices contained in the same physical device. *RemoteUIServer* service may be dependent on the *DeviceSecurity* service for providing access control to the actions defined in the services.

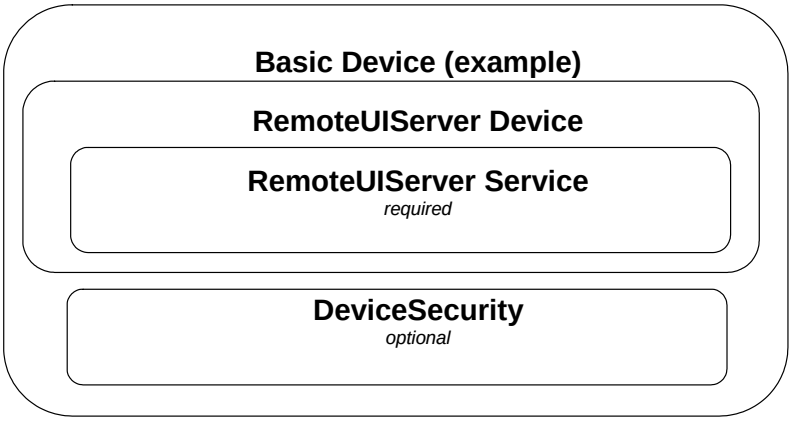

Figure 2: Example of *DeviceSecurity* outside *RemoteUIServerDevice*

2.2.2. Relationships Between Services

The dependencies between the services are listed in the above section under the possible models of implementing services in *RemoteUIServerDevice*.

2.3. Theory of Operation

It is highly recommended for the Remote UI server to use *DeviceSecurity* service to secure specific UPnP™ Remote UI server actions. This section assumes that the reader has an overall understanding of UPnP™ Security. Please refer to the *DeviceSecurity*:1 Service Control Specification for detailed description of a secure UPnP™ device.

2.3.1. Secure Remote UI Servers (if DeviceSecurity implemented in Remote UI server device)

RemoteUIServer service provides a set of actions to give a list of user interfaces and to destroy an unconnected, instantiated UI. The actions in this service that change the device state should be authenticated via UPnP™ security. Some actions in *RemoteUIServer* service can carry critical information such password as arguments. By using *DecryptAndExecute* action defined in *DeviceSecurity* service, security sensitive information can be protected . A control point that accesses the secure actions on the service has to be initially authenticated via a Security Console application as described in UPnP™ Security DCP. Access control definitions such as Permissions, Profiles and Access Control List(ACL) for Remote UI server device are described in Appendix A.

3. XML Device Description

```
<?xml version="1.0" encoding="UTF-8"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
    <specVersion>
        <major>1</major>
        <minor>0</minor>
    </specVersion>
    <URLBase>base URL for all relative URLs</URLBase>
    <device>
        <deviceType>urn:schemas-upnp-org:device:RemoteUIServerDevice:1
</deviceType>
        <friendlyName>short user-friendly title</friendlyName>
        <manufacturer>manufacturer name</manufacturer>
        <manufacturerURL>URL to manufacturer site</manufacturerURL>
        <modelDescription>long user-friendly title</modelDescription>
        <modelName>model name</modelName>
        <modelNumber>model number</modelNumber>
        <modelURL>URL to model site</modelURL>
        <serialNumber>manufacturer's serial number</serialNumber>
        <UDN>uuid:UUID</UDN>
        <UPC>Universal Product Code</UPC>
        <iconList>
            <icon>
                <mimetype>image/format</mimetype>
                <width>horizontal pixels</width>
                <height>vertical pixels</height>
                <depth>color depth</depth>
                <url>URL to icon</url>
            </icon>
        </iconList>
        <serviceList>
            <service>
                <serviceType>urn:schemas-upnp-org:service:RemoteUIServer:1</serviceType>
                <serviceId>urn:upnp-org:serviceId:RemoteUIServer</serviceId>
                <SCPDURL>URL to service description</SCPDURL>
                <controlURL>URL for control</controlURL>
                <eventSubURL>URL for eventing</eventSubURL>
            </service>
        </serviceList>
        <presentationURL>URL for presentation</presentationURL>
    </device>
</root>
```

4. Test

No semantic tests are defined for this device.

Annex A
(normative)

Access Control Definitions
(if *DeviceSecurity* service is implemented)

This section specifies the Permissions, Profiles and Access Control List (ACL) entry to be implemented in the *DeviceSecurity* service that can optionally be used by the *RemoteUIServerDevice*. This is used by the Security Console to assign access control of secure actions on the Remote UI server device to control point applications. Please refer to the *DeviceSecurity1.0* service specification for more details about Security Console, Permissions, Profiles and ACLs.

A.1 Permissions

The following table describes the permissions to perform access control on the secure actions of the services embedded in the Remote UI server device. The *RUISDeviceAll* is a required permission which can securely access all actions in the *RemoteUIServer* service. The other permissions are optional. Vendors may define additional set of permissions to perform access control on the Remote UI client device. For example, they may provide separate master and guest permissions for the finer granularity of access. However, for better interoperability, vendors should use the optional permissions presented in this document than implementing their own security permissions.

Table 4: Defined permissions for *RemoteUIServer* Service

Permission	Allowed Actions
RUISDeviceAll[1]	*All actions in RemoteUIServer Service.*
RUISDeviceInfo	*GetCompatibleUIs*
RUISDeviceChangeStatus	*SetUILifetime*

[1] *RUISDeviceAll* must be implemented.

When implementing only one the required *RUISDeviceAll* permission, the following XML format is used:

```
<Permission>
        <UIname>RUISDeviceControl</UIname>
        <ACLEntry>
                <RUIWG:RUISDeviceAll/>
        </ACLEntry>
        <FullDescriptionURL></FullDescriptionURL>
        <ShortDescription>
                This permission allows the control point to set and get all secure actions
                of all the services of the Remote UI server device.
        </ShortDescription>
</Permission>
```

XML element tags UIname, ACLEntry, FullDescription, ShortDescription and Permission are defined in *DeviceSecurity1*.0 service specification.

The above defined permission is returned by the Remote UI server device in the “DefinedPermissions” argument of *DeviceSecurity*’s GetDefinedPermission action.

If the *DeviceSecurity* service resides **inside** the *RemoteUIServerDevice*, it will contain only the defined permissions of the Remote UI server device (as mentioned above). The “DefinedPermissions” argument of GetDefinedPermission action returned by the *DeviceSecurity* in this case would be:

```
<DefinedPermissions>
        <Permission>
                <UIname>RUISDeviceControl</UIname>
                <ACLEntry>
                        <RUIWG:RUISDeviceAll/>
                </ACLEntry>
                <FullDescriptionURL></FullDescriptionURL>
                <ShortDescription>
                        Allow this application to complete control of the Remote UI server device.
                </ShortDescription>
        </Permission>
</DefinedPermissions>
```

If the *DeviceSecurity* service resides **outside** of the *RemoteUIServerDevice* and the *RemoteUIServerDevice* is embedded in a container device with other devices such as *MediaRenderer*, the “DefinedPermissions” argument of GetDefinedPermission action returned by the *DeviceSecurity* service in this case would be:

```
<DefinedPermissions>
        <Permission>
                <UIname>RUISDeviceControl</UIname>
                <ACLEntry>
                        <RUIWG:RUISDeviceAll/>
                </ACLEntry>
                <FullDescriptionURL></FullDescriptionURL>
                <ShortDescription>
                        Allow this application to complete control of the Remote UI server device.
                </ShortDescription>
        </Permission>
        <Permission>
                e.g., Permission defined by MediaRenderer Device
        </Permission>
…
</DefinedPermissions>
```

A.2 Profiles

There is no profile specified to be used for the Remote UI server device. However, vendors may define profiles of their own. Please refer to *DeviceSecurity*1.0 service specification for more details.

A.3 Access Control List (ACL) entry

If DeviceSecurity service is implemented in the UPnP™ Remote UI server device, *RemoteUIServer* would have the “<RUIWG:RUISDeviceAll>” defined permission for access control. Following XML shows an example ACL entry granting this defined permission to the control point specified in the subject element**.** The string value “dRDPBgZz…” under the <hash> tag denotes the public key hash of the control point for which this ACL is defined as an example.

```
<acl>
        <entry>
                <subject>
                        <hash>
                                <algorithm>SHA1</algorithm>
                                <value>dRDPBgZzTFq7Jl2Q2N/YNghcfj8=</value>
                        </hash>
                </subject>
                <access>
                        <RUIWG:RUISDeviceAll/>
                </access>
                <valid>
                        <not-before>2002-10-23_05:17:32</not-before>
                        <not-after>2004-12-31_23:59:59</not-after>
                </valid>
        </entry>
</acl>
```

ICS 35.200

Price based on 9 pages