RemoteUiClientDevice:1 Device Template Version 1.01

For UPnP Version 1.0
Status: Standardized DCP
Date: April 16, 2014

This Standardized DCP has been adopted as a Standardized DCP by the Steering Committee of the UPnP Forum, pursuant to Section 2.1(c)(ii) of the UPnP Forum Membership Agreement. UPnP Forum Members have rights and licenses defined by Section 3 of the UPnP Forum Membership Agreement to use and reproduce the Standardized DCP in UPnP Compliant Devices. All such use is subject to all of the provisions of the UPnP Forum Membership Agreement.

THE UPNP FORUM TAKES NO POSITION AS TO WHETHER ANY INTELLECTUAL PROPERTY RIGHTS EXIST IN THE STANDARDIZED DCPS. THE STANDARDIZED DCPS ARE PROVIDED "AS IS" AND "WITH ALL FAULTS". THE UPNP FORUM MAKES NO WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE STANDARDIZED DCPS, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OF REASONABLE CARE OR WORKMANLIKE EFFORT, OR RESULTS OR OF LACK OF NEGLIGENCE.

© 2014 UPnP Forum. All Rights Reserved.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ylian Saint-Hilaire</td>
<td>Intel Corporation</td>
</tr>
<tr>
<td>Mark Walker</td>
<td>Intel Corporation</td>
</tr>
<tr>
<td>Ku Bong Min</td>
<td>LG Electronics</td>
</tr>
<tr>
<td>Richard Bardini</td>
<td>Intel Corporation</td>
</tr>
</tbody>
</table>
Contents

1. OVERVIEW AND SCOPE......................................................................................................................... 3
2. DEVICE DEFINITIONS............................................................................................................................... 4
   2.1. DEVICE TYPE........................................................................................................................................ 4
   2.2. DEVICE MODEL................................................................................................................................... 4
       2.2.1. Description of Device Requirements.......................................................................................... 4
       2.2.2. Relationships Between Services.................................................................................................. 6
   2.3. THEORY OF OPERATION..................................................................................................................... 6
       2.3.1. Secure Remote UI Clients (if DeviceSecurity implemented in Remote UI client device)... 6
3. XML DEVICE DESCRIPTION...................................................................................................................... 7
4. TEST .......................................................................................................................................................... 8

APPENDIX A: ACCESS CONTROL DEFINITIONS (IF DEVICESECURITY SERVICE IS IMPLEMENTED)......................................................................................................................... 9
   A1 PERMISSIONS....................................................................................................................................... 9
   A2 PROFILES.......................................................................................................................................... 10
   A3 ACCESS CONTROL LIST (ACL) ENTRY............................................................................................... 10

List of Tables

Table 1: RemoteUIClientDevice Service Descriptions .................................................................................. 4
Table 2: Device Requirements for stand-alone RemoteUIClientDevice .......................................................... 4
Table 3: Device Requirements for embedded RemoteUIClientDevice .......................................................... 5
Table 4: Defined permissions for RemoteUIClient Service ............................................................................ 9

© 2014 UPnP Forum. All Rights Reserved.
1. Overview and Scope

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

This document defines the device

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

The RemoteUIClientDevice encapsulates all services for the Remote UI Client Device Control Protocol (DCP).
2. Device Definitions

2.1. Device Type

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

\[ \text{urn:schemas-upnp-organizzation:device:RemoteUI\text{ClientDevice}:1} \]

2.2. Device Model

It is recommended that RemoteUI\text{ClientDevice} 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 RemoteUI\text{ClientDevice} implementation or in a device that encompasses the RemoteUI\text{ClientDevice}. These two models are described below.

2.2.1. Description of Device Requirements

The following table briefly describes the services used in RemoteUI\text{ClientDevice}.

**Table 1: RemoteUI\text{ClientDevice} Service Descriptions**

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteUI\text{Client}</td>
<td>Allows for basic operations on a Remote UI client including: user interface connection management, optionally user interface availability management and optionally basic user interaction.</td>
</tr>
<tr>
<td>DeviceSecurity</td>
<td>Actions for taking ownership, configuring access control, establishing secure sessions, and invoking secure actions.</td>
</tr>
</tbody>
</table>

2.2.1.1. DeviceSecurity within RemoteUI\text{ClientDevice}

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

**Table 2: Device Requirements for stand-alone RemoteUI\text{ClientDevice}**

<table>
<thead>
<tr>
<th>DeviceType</th>
<th>Root</th>
<th>Req. or Opt.</th>
<th>ServiceType</th>
<th>Req. or Opt.</th>
<th>Service ID^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteUI\text{ClientDevice}:1</td>
<td>Yes</td>
<td>R</td>
<td>RemoteUI\text{Client}:1</td>
<td>R</td>
<td>RemoteUI\text{Client}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeviceSecurity:1</td>
<td>O</td>
<td>DeviceSecurity</td>
</tr>
<tr>
<td>Non-standard services</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>To be defined by vendor</td>
</tr>
</tbody>
</table>

^1 R = Required, O = Optional, X = Non-standard.  
^2 Prefixed by urn:upnp-organizzation: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 clients.

Figure 1: DeviceSecurity within RemoteUI_CLIENTDevice

2.2.1.2. DeviceSecurity outside RemoteUI_CLIENTDevice

This model is typically applicable to physical devices that implement Remote UI Client functionality, but the RemoteUI_CLIENTDevice may use DeviceSecurity that is already part of another device. An example of this would be where urn:schemas-upnp-org:device: RemoteUI_CLIENTDevice: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 RemoteUI_CLIENTDevice must contain the minimum version number of the service specified in the table below.

Table 3: Device Requirements for embedded RemoteUI_CLIENTDevice

<table>
<thead>
<tr>
<th>DeviceType</th>
<th>Root</th>
<th>Req. or Opt.¹</th>
<th>ServiceType</th>
<th>Req. or Opt.¹</th>
<th>Service ID²</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteUI_CLIENTDevice:1</td>
<td>Yes</td>
<td>R</td>
<td>RemoteUI_CLIENT:1</td>
<td>R</td>
<td>Non-standard services embedded by an UPnP vendor go here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

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 clients that may use the DeviceSecurity service for other UPnP™ devices contained in the same physical device. RemoteUI_CLIENT service may be dependent on the DeviceSecurity service for providing access control to the actions defined in the services.
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 RemoteUIClientDevice.

2.3. Theory of Operation

A Remote UI client can be a fully autonomous device that runs its own user interface in addition to executing remoted UIs, or it may be a fully remoted device with no local UI capability. In both cases, the RemoteUIClientDevice:1 UPnP device is implemented, allowing anyone on the network to discover and control the Remote UI client. Since many different types of user interaction device exist with many different form factors and usages, the behavior of the Remote UI client device may change.

In any case, it is highly recommended for the Remote UI client to employ the DeviceSecurity service to secure specific UPnP™ Remote UI client 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 Clients (if DeviceSecurity implemented in Remote UI client device)

RemoteUIClient service provides a set of actions to manage remote connections and process user’s input data. The actions in this service that change the device state should be authenticated via UPnP™ Security. Some actions in RemoteUIClient service can carry critical information such as password in their argument field. 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 client device are described in Appendix A.
3. **XML Device Description**

```xml
<?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:RemoteUIClientDevice: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:RemoteUIClient:1</serviceType>
        <serviceId>urn:upnp-org:serviceId:RemoteUIClient</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._
Appendix A: 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 RemoteUIClientDevice. This is used by the Security Console to assign access control of secure actions on the Remote UI client device to control point applications. Please refer to the DeviceSecurity1.0 service specification for more details about Security Console, Permissions, Profiles and ACLs.

A1 Permissions

The following table describes the permissions to perform access control to the secure actions of the services embedded in the Remote UI client device. The RUICDeviceAll is a required permission which can securely access all the actions in the RemoteUIClient 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 finer granularity of access. However for maximum interoperability, vendors should use the optional permissions presented in this document rather than implementing their own security permissions.

Table 4: Defined permissions for RemoteUIClient Service

<table>
<thead>
<tr>
<th>Permission</th>
<th>Allowed Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUICDeviceAll</td>
<td>All actions in RemoteUIClient Service.</td>
</tr>
<tr>
<td>RUICDeviceInfo</td>
<td>GetCurrentConnections, GetDeviceProfile, GetUIListing</td>
</tr>
<tr>
<td>RUICDeviceChangeConnection</td>
<td>Connect, Disconnect</td>
</tr>
<tr>
<td>RUICDeviceChangeStatus</td>
<td>AddUIListing, RemoveUIListing, DisplayMessage, ProcessInput</td>
</tr>
</tbody>
</table>

RUICDeviceAll must be implemented.

When implementing only the required RUICDeviceAll permission, the following XML format is used:

```xml
<Permission>
    <UName>RUICDeviceControl</UName>
    <ACLEntry>
        <RUIWG:RUICDeviceAll/>
    </ACLEntry>
    <FullDescriptionURL/>
    <ShortDescription>
        This permission allows the control point to set and get all secure actions of all the services of the Remote UI client device.
    </ShortDescription>
</Permission>
```

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

The above defined permission is returned by the Remote UI client device in the “DefinedPermissions” argument of DeviceSecurity’s GetDefinedPermission action.
If the DeviceSecurity service resides inside the RemoteUI/ClientDevice, it will contain only the defined permissions of the Remote UI client device (as mentioned above). The “DefinedPermissions” argument of GetDefinedPermission action returned by the DeviceSecurity in this case would be:

```xml
<DefinedPermissions>
  <Permission>
    <UName>RUICDeviceControl</UName>
    <ACLEntry>
      <RUIWG:RUICDeviceAll/>
    </ACLEntry>
    <FullDescriptionURL></FullDescriptionURL>
    <ShortDescription>
      Allow this application to complete control of the Remote UI client device.
    </ShortDescription>
  </Permission>
</DefinedPermissions>
```

If the DeviceSecurity service resides outside of the RemoteUI/ClientDevice and the RemoteUI/ClientDevice 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:

```xml
<DefinedPermissions>
  <Permission>
    <UName>RUICDeviceControl</UName>
    <ACLEntry>
      <RUIWG:RUICDeviceAll/>
    </ACLEntry>
    <FullDescriptionURL></FullDescriptionURL>
    <ShortDescription>
      Allow this application to complete control of the Remote UI client device.
    </ShortDescription>
    <Permission>
      e.g., Permission defined by MediaRenderer Device
    </Permission>
  ...  
</DefinedPermissions>
```

### A2 Profiles

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

### A3 Access Control List (ACL) entry

If DeviceSecurity service is implemented in the UPnP™ Remote UI client device, RemoteUI/Client would have the “<RUIWG:RUICDeviceAll>” 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.

```xml
<acl>
```

---

10
<entry>
  <subject>
    <hash>
      <algorithm>SHA1</algorithm>
      <value>dRDPBgZzTFq7Jl2Q2N/YNghcjf8=</value>
    </hash>
  </subject>
  <access>
    <RUIWG:RUICDeviceAll/>
  </access>
  <valid>
    <not-before>2002-10-23_05:17:32</not-before>
    <not-after>2004-12-31_23:59:59</not-after>
  </valid>
</entry>