Device Discovery, Authentication, and Pairing

Published 2014-10-28 | (Compatible with SDK 3.5,4.5,5.0,5.1 and 2012,2013,2014 models)

> Device Discovery, Authentication, and Pairing

Contents

Device Discovery

Device discovery is done via the SSDP protocol (Simple Service Discovery Protocol), defined by the UPnP standard. When a device is added to the network, SSDP allows the device to advertise its services to control points on the network. When a control point is added to the network, SSDP allows that control point to search for devices of interest on the network. The fundamental exchange in both cases is a discovery message containing essential specifics about the device or one of its services.

This document defines a simple way for a mobile device to discover Samsung smart TV supporting Smart View service on the network. The mobile device (Client application developed by the application developer) acts as a Control Point. Devices are discovered via the SSDP M-SEARCH method, using a below specific search target (ST) header.

MSearch ST: urn:samsung.com:service:MultiScreenService:1

TV devices that implement the service specified in the search target (ST) field will respond with HTTP/1.1 200 OK and URL of the device description.

LOCATION: http://<TV ip address>:<TV port number></path>/description.xml

2nd screen app requests the device description by issuing a GET request on the LOCATION URL. 1st screen devices will respond with resource URL. (http://TV IP/Port/base URL)

HTTP/1.1 200 OK

Application-URL: http://192.168.1.52:80/ws/apps/

At this point, the mobile device knows TV devices that support Smart View service and TV IP address. (When connecting to TV, this IP is used)

Once the mobile device has the URL, it requests the device description by issuing a GET request on the URL. The mobile device then parses the description.xml file to extract friendly name of TV.

```
<root>
  ...
  <device>
  ...
    <friendlyName>[TV]Name</friendlyName>
  </device>
</root>
```

Device Authentication and Pairing

After discovery:

1. The mobile device sends a POST message with the MAC address, IP address, and device name to the TV for connection.

2. The TV authenticates the mobile device using the MAC address. If the authentication is successful, the mobile can connect.

   The first time users attempt to pair their mobile device with the TV, the TV displays a Popup message prompting users to select either:

   Allow pairing If the user selects **Allow** , the mobile device can successfully authenticate and connect with Tv App.
   Deny pairing If user can selects **Deny** , the mobile device fails to authenticate and cannot connect with TV App.

The authentication the response messages from the TV to the mobile device are as follows:

1. When the user selects **Allow** , the TV sends an **Authentication Success** response message to the mobile device. After that, the mobile device can connect to the TV.

   HTTP Response Message = OK (200)
2. When the user selects **Deny** , TV sends an **Authentication Failure** response message to mobile device. After that, the mobile device displays a **Authentication Failure** message and disconnects with the TV the mobile device no longer displays **Denied TV** in the TV list.

   HTTP Response Message = UNAUTHORIZED (401) or NOTFOUND(404)
3. When the user tries to connect 5 devices with the TV simultaneously, the TV sends a HTTP response message for full connection to mobile device. After that, the mobile device can display a **Full connection** message and disconnect from the TV.

   HTTP Response Message = SERVICEUNAVAILABLE (503)
4. When the user does not select allow or deny, the TV closes the popup message and sends a “Authentication Timeout” response message to mobile device. After that, mobile device displays a **Authentication Timeout** message.

   HTTP Response Message = UNAUTHORIZED (401) or NOTFOUND(404)
5. When the user enters the Network Menu (Menu -> Network -> AllShare Settings) and deletes or denies the mobile device, TV sends a HTTP response message for deletion or denial to the mobile device.

   HTTP Response Message = UNAUTHORIZED(401) or NOTFOUND(404)