UPNP® DEVICE MANAGEMENT— SIMPLIFY THE ADMINISTRATION OF YOUR DEVICES

April 2011

MANAGEMENT SUMMARY

Problem statement

Today more and more devices are connected to Internet. TVs, smartphones, tablets, printers, picture frames, cameras and other consumer devices are part of people's day to day life. These devices run different execution environments, such as OS platforms and virtual machines. In such a heterogeneous and connected environment, some form of management is required for the devices to work together, enabling services for users and consumer satisfaction. It is required to do local or distant updates when new releases of software and firmware are available and should be updated to avoid recall or to enable a new application or service. Discovering device capabilities and applying a correct configuration is required for enabling connectivity and services. Doing such configuration remotely makes it easy for the users. It is also required to perform diagnosis to ensure enhanced experience for users. In addition to such common management functions, there can be device specific requirements.

An open standard solution for management would provide a common set of interfaces, management action definitions and data models for devices in various environments. It can also extend remote management solutions.

Solution description

UPnP Device Management provides a common solution through defining standard management actions and data models, which can be implemented in devices running different execution environments. UPnP DM also allows defining new data models for specific device usage.

CONTENTS

REFERENCES

- [BMS] UPnP DM Basic Management:1 Service Template, for UPnP version 1.0, July 2010, http://upnp.org/specs/dm/UPnP-dm-BasicManagement-v1-Service.pdf.
- [Bonjour] Management protocol defined by Apple, http://www.apple.com/support/bonjour/.
- [CMS] UPnP DM Configuration Management:1 Service Template, for UPnP version 1.0, July 2010, http://upnp.org/specs/dm/UPnP-dm-ConfigurationManagement-v1-Service.pdf.
- [CWMP] Customer premise equipment WAN Management Protocol, http://www.broadband-forum.org/cwmp.php.
- [DPS] UPnP Device Protection:1 Service Template, for UPnP version 1.0, March 2011, http://upnp.org/specs/gw/deviceprotection1.
- [DPWS] Device Profile for Web Service, July 2009, http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01.
- [OMA-DM] Open Mobile Alliance, Device Management, http://www.openmobilealliance.org/Technical/DM.aspx.
- [SMS] UPnP DM Software Management:1 Service Template, for UPnP version 1.0, July 2010, http://upnp.org/specs/dm/UPnP-dm-SoftwareManagement-v1-Service.pdf.
- [SNMP] Simple Network Management Protocol, http://www.rfc-editor.org/rfc/std/std62.txt.
- [UDA] UPnP Device Architecture 1.1, October 2008, http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf.
- [UMD] UPnP DM Manageable Device:1 Device Template, for UPnP version 1.0, July 2010, http://upnp.org/specs/dm/UPnP-dm-ManageableDevice-v1-Device.pdf.
- [UWP] UPnP white paper, September 2010, http://upnp.org/resources/whitepapers/UPnPWhitePaper_2010.pdf.

INTRODUCTION TO UPNP

Universal Plug and Play is a set of networking protocols proposed by the UPnP Forum (www.upnp.org).

The goal of UPnP technology is to provide a broad industry initiative that simplifies networking for small businesses and consumers. It intends to easily connect computers and other devices into a network 'hub' from which to access data, transport media and offer network connectivity under the command of any connected control device.

UPnP device control protocols (DCP) are built upon open, Internet-based communication standards and can therefore be implemented on any operating system. It works with any type of physical networking media that supports IP, wired or wireless, and offers a multitude of options.

UPnP devices are "plug-and-play" in that when connected to a network they automatically announce their network address and supported device and services types, enabling clients that recognize those types to immediately begin using the device.

Any Control Point (CP) connected to the LAN will broadcast search requests to identify available UPnP devices and their supported actions. Control Point can then start invoking these discovered actions. Actions invoked will initiate asynchronous operations and return operation IDs via which results can subsequently be obtained.

UPnP device and service standards are defined and published for Internet gateways/routers, audio-video media devices, printers, scanners, climate control, lighting and wireless LAN access points, digital security cameras, and advanced features such as security, remote user interface and quality of service.

There are various device control protocols such as Internet Gateway Device (UPnP IGD), Audio and Video (UPnP AV, upon which DLNA is partially based), Remote Access (UPnP RA) and Device Management (UPnP DM).

For more information, UPnP Forum has published a UPnP white paper in September 2010 [UWP].

DEVICE MANAGEMENT

Device Management refers to the mechanism of managing devices on a network. It involves provisioning and configuration services, updating software/firmware, diagnosing faults etc.

Device Management enables users, service providers, and manufacturers to manage their devices and services. A Device Management framework requires the definition of data models corresponding to the parameters being managed, management actions as well as protocols for the exchange of management actions and data.

There are various local or remote management solutions available depending on markets and manufacturers:

- Telecom Operators tend to support remote solution such as [CWMP] (CPE WAN Management Protocol a.k.a. TR-069).
- Telco legacy systems also rely on Simple Network Management Protocol [SNMP] and Management Information Base (MIB) that describe device data structure.
- Apple is providing its own local solution called [Bonjour] that is not only focused on management.
- Some Home automation vendors are looking at [DPWS] with the addition of WS-Management for local or remote operations.

UPnP Device Management 1.0 specifications have been published by the UPnP Forum in 2010. It has been developed over more than 3 years by a UPnP Working Committee composed of experts from consumer Electronic manufacturers, telecom equipment providers and telecom service providers. Due to the proposed concepts and its contributor profile, UPnP Device Management is particularly adapted for the management of residential IP connected equipment.

UPNP DEVICE MANAGEMENT OVERVIEW

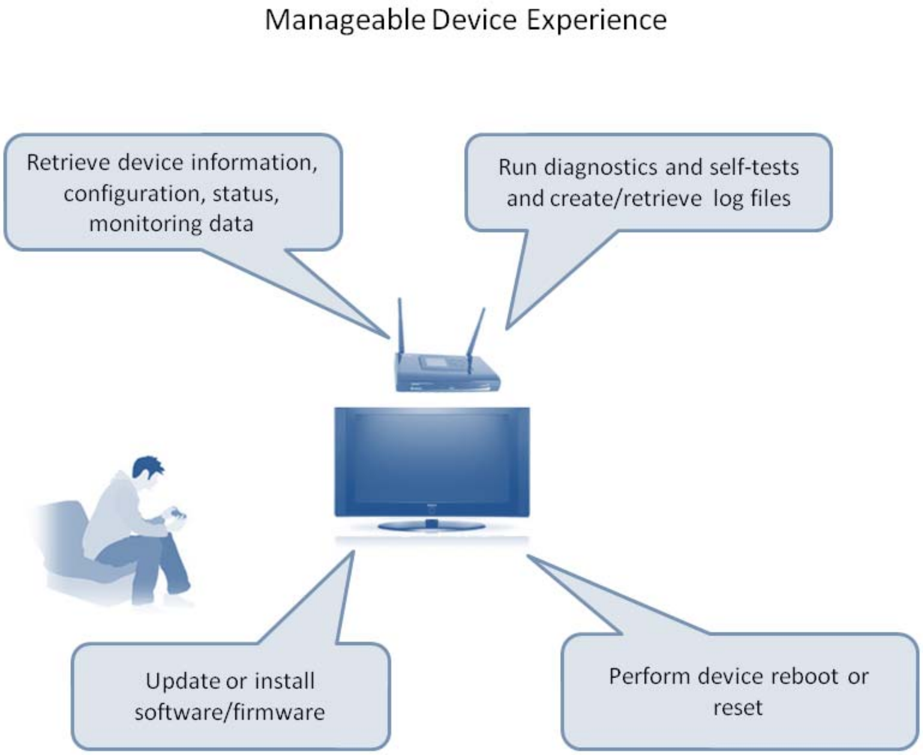
UPnP Device Management (UPnP DM) is a DCP which defined three services to address management operations to any UPnP device’s Execution Environment (e.g. OS, virtual machines or scripting engines). A full-featured UPnP DM device provides control points with the following capabilities:

- Basic Management: the service is designed for rebooting and/or resetting the device, performing IP (Internet Protocol) layer and self-test diagnostics, retrieving the status of the device and reading the content of device logs.
- Configuration Management: the service is designed for reading the configuration and the status of the device, provisioning and configuring services.
- Software Management: the service is designed for the management of the lifecycle of the device software components and firmware images.

The protocol for the communication between the management agents and devices are specified in the [UDA] specification.

An UPnP MD corresponds to a physical or a virtual device with an associated data model and a number of potentially software entities to be managed. A data model represents the states of various device aspects and can be used to retrieve status information as well as to control the functions of a device. Description of a Manageable Device is specified in the UPnP Manageable Device [UMD] specifications. It describes the device type, manufacturer, model, serial number, Universal Product Code (UPC), supported UPnP DM Services etc.

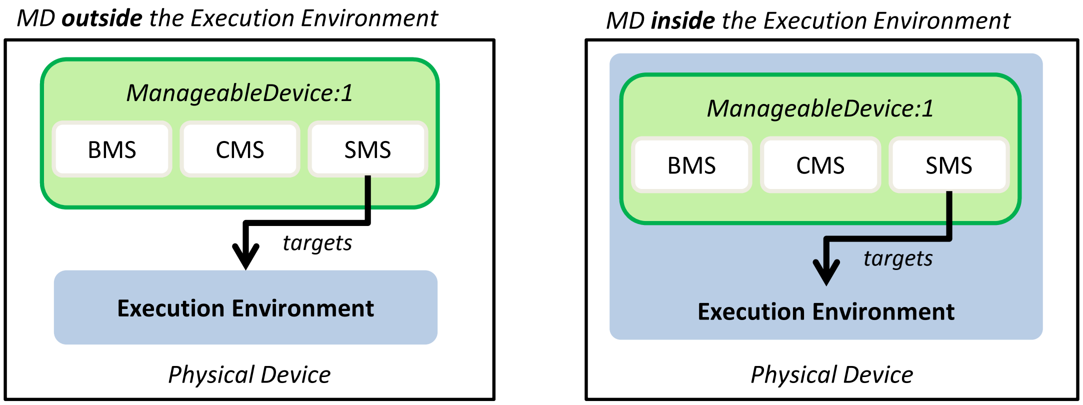
UPnP MD is specified so that it is a flexible solution. Its implementation on each device depends on manufacturer decision. In other words, implementers are free to decide which optional actions they want to support and which additional specific extensions they want to add to the manageable device data model.


Manageable Device Experience
Retrieve device information, configuration, status, monitoring data
Run diagnostics and self-tests and create/retrieve log files
Update or install software/firmware
Perform device reboot or reset

DEPLOYMENT OPTIONS OF UPNP DM

An execution environment (EE) can be thought of as a physical or virtual machine. For example, the operating system is an EE, and so is any Java virtual machine or scripting engine. A physical device (PD) that hosts multiple EEs might host more than one manageable device (MD).

Relationship between Manageable Device (MD) and Execution Environment



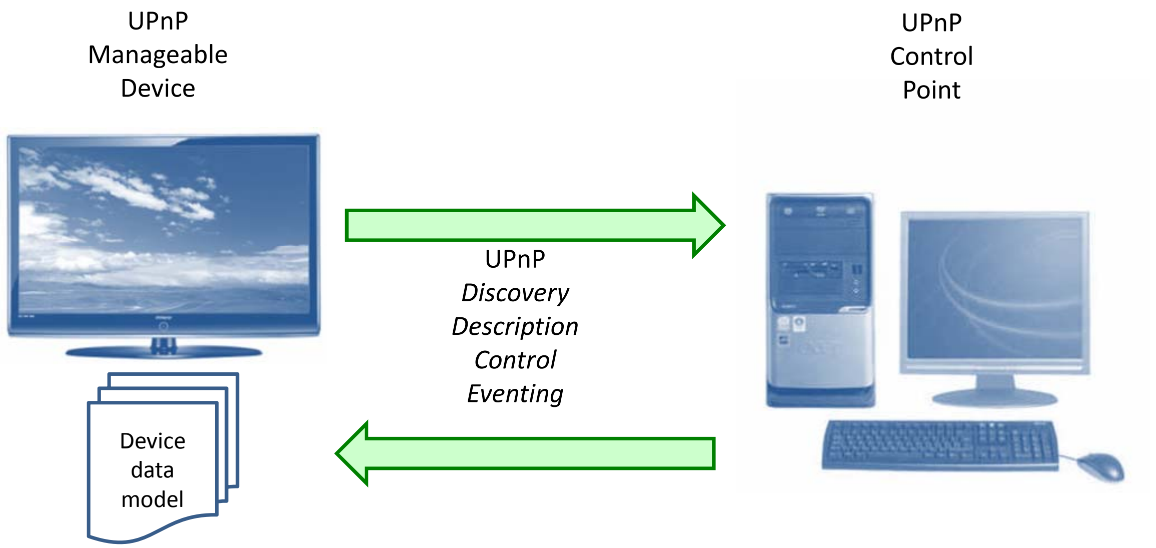
The specification defines various deployment scenarios as listed below:

- The Manageable Device is the unique instance closest to the physical device.
- Multiple UPnP devices are available in a single physical device and one of these is the Manageable Device.
- The Manageable Device is embedded within another UPnP device.
- The Manageable Device is embedding other UPnP devices.
- Deployment where some of the previous deployment options are mixed.

LOCAL AND REMOTE MANAGEMENT APPLICATIONS OF UPNP DM

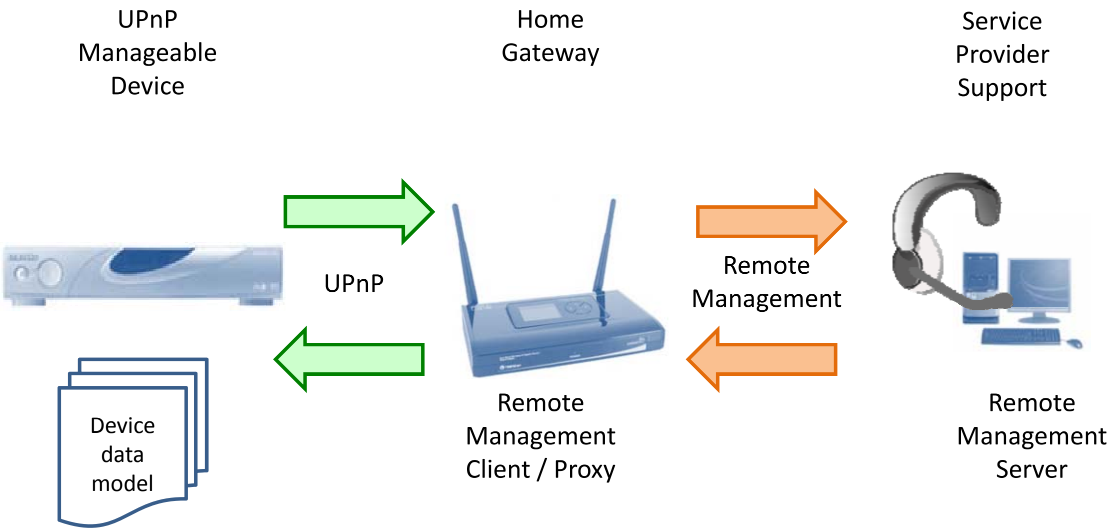
UPnP Device Management can be used within a local IP network to provide management operation for local users.

Local Management of Devices in a Home Network



But UPnP DM operations can also be used from outside via any remote access protocol using a local proxy gateway from the remote management protocol to UPnP.

Remote Management of Devices



Such a remote management implementation will require the implementation of a proxy between UPnP DM and a remote management protocol. This could be, for instance, based on [CWMP] (a.k.a. TR-069) or UPnP Remote Access. In fact UPnP DM proposes mappings to [CWMP], [OMA-DM] and [SNMP] protocols.

UPNP DM SPECIFICATION DOCUMENTS

The UPnP Device Management:1 specifications have been published by UPnP Forum on July 2010. It includes the following specifications:

- Manageable Device – The specification provides architectural concepts for the deployment of UPnP DM [UMD].
- Basic Management Service – This mandatory service provides basic management actions such as reboot, reset, diagnostics and access to log information. [BMS].
- Configuration Management Service – This is a mandatory service that provides generic management actions for accessing and manipulating parameters exposed by the device through UPnP DM data models [CMS].
- Software Management Service – This optional service provides actions to manage software (including firmware) in devices [SMS].

The UPnP DM Working Committee is now focused on boosting security for UPnP Device Management:2 planned to be released in Q3 2011.

DATA MODELS

UPnP DM abstracts manageable parameters provided by the device through a Data Model framework.

A set of Common Objects is defined as a minimum mandatory data model. It includes device Information, such as hardware version and network interface parameters. It provides the flexibility for device vendors to define data model for custom functionalities supported by their devices. It also allows mapping of data models from other management standards to the UPnP DM data model.

Parameters in the data model are designed using a hierarchical structure like a logical tree, quite similar to directories and files in a file system.

Using Configuration Management Service [CMS], a control point can read and write their values by specifying a name that uniquely identifies the parameter. In addition to the read and write operations on parameters, a control point can also create and delete instances of objects from templates in a similar way as rows of a data table can be created or deleted.

UPNP DM SERVICES

Once a control point discovers UPnP-enabled devices that implement UPnP DM services (a.k.a. manageable devices), it can perform various management actions on these devices and manage parameters exposed in the form of data models. The three UPnP DM services are briefly described below.

Basic Management Service

The Basic Management Service [BMS] specifies management actions for device maintenance, diagnostics and logging as well as device management actions such as reboot, baseline reset, self-test execution in order to diagnose problems, and log management (enable, disable and retrieve log information).

The management actions and associated state variables are define in the Basic Management Specification.

- Reboot and baseline reset result in specific operations of the device.
- Other basic management actions return the current value of state variables associated with the action.

The action that returns the device status is the only one mandatory for Basic Management.

Configuration Management Service

The Configuration Management Service [CMS] allows the control point to manipulate configuration parameters in devices and is mandatory for devices supporting UPnP DM.

CMS defines the action to manage the parameters exposed by the device in terms of supported data model. The data model is a hierarchical tree starting with a root node. Parameters in the data model can be uniquely identified and addressed. Because CMS specifies the Common Objects data model and is a mandatory service, control points can assume that all manageable devices will implement CMS and support the Common Objects.

CMS specifies device actions such as discovering of a data model and current instances, data model manipulation (read, write, create, delete), get or retrieve values, get and set parameter's attributes, event on parameter value change, create or delete multi-instance objects instances. Of these actions, only read access to the data model is mandatory:

- Data Model Discovery – retrieve information about supported data models, parameters and instances.
- Reading and writing of parameter values – get and set values from and to a data model.
- Reading and writing of attribute values – get and set attributes of nodes in a data model.
- Creating and deleting instances (table rows) – Create/Delete object instances.

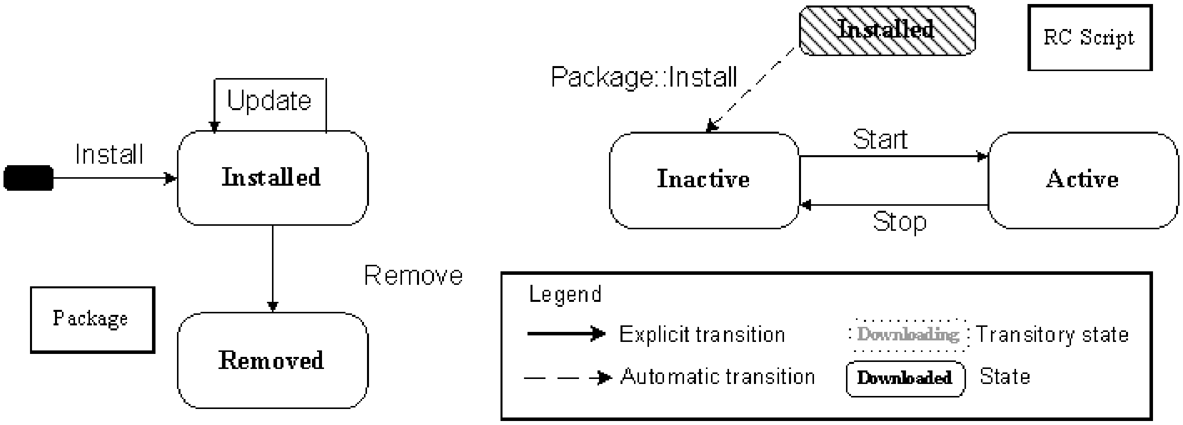
CMS actions allow the discovery of supported data models in a device and the manipulation of parameters in any data model. CMS Data Model supports parameters for device info, physical device, device ID, network interfaces, network configuration (IPv4, IPv6, OS, etc.).

CMS also specifies mapping rules for TR-069 (CWMP defined by Broadband Forum), OMA-DM (Open Mobile Alliance) and MIB (SNMP). CMS supports the action to retrieve supported data models in a device, both UPnP DM data models and those defined by other organizations.

Software Management Service

The Software Management Service [SMS] enables a UPnP DM Control Point to manage software entities and firmware present in an Execution Environment of a device supporting UPnP DM.

Example of Execution Environment
with Deployment Units and Execution Units



Software entities can either be Deployment Units or Execution Units:

- A Deployment Unit (DU) is a package of related software modules and other resources, such as executable files, library files, configuration files, jar files, bundles or assemblies, which is deployed to an execution environment as a single package.

- An Execution Unit (EU) is a software entity that can be individually started or stopped, such as script, virtual machine applications, etc. An EU provides a service. Each EU is linked to a single Deployment Unit, however one Deployment Unit can include multiple Execution Units.

SMS does not specify a download mechanism. Any existing protocol can be used by implementers for the actual download of Deployment Units. This usually depends on the Execution Environment's technology used to install software packages.

SMS specifies actions that can be performed on Deployment Units and Execution Units. It also provides a standard data model which contains details of these entities. For example, the data model includes information on dependency between software entities and the ability of the Execution Environment to handle these dependencies.

SMS actions include install, update, uninstall on Deployment Units (including the firmware), start and stop on Execution Units, retrieve status information etc.

The SMS Data Model supports parameters related to the software capabilities of the execution environment (ability to start/restart, handle DU/EU dependencies), information on all DUs and EUs.

UPNP DM USE CASES

There are many examples for use case that may require UPnP Device Management; here are some real life scenarios:

- John owns a TV and purchase an additional webcam hardware module compatible with its TV set. He now wants to enable the video conferencing service. To do so, the TV software must be upgraded to support the new video conferencing features. John will use a manufacturer UPnP Control Point on his computer and using a local GUI, he will trigger the automatic installation of a new software package on his TV set, using UPnP DM SMS actions. Now he will be able, with this Control Point, to configure the necessary setting to enjoy his Video conferencing service, using UPnP DM CMS actions.
- Maria just bought a new VoIP phone compatible with her VoIP service provider. However when she tries to use the phone, she always get an error message stating that connection to the VoIP server cannot be established. Using the Control Point provided by her service provider on her PC, Maria triggers a diagnostic test. The Control Point (CP) will then start a series of tests, for example VoIP Phone self-test, Ping from VoIP Phone to VoIP server, DNS lookup or bandwidth test using UPnP DM BMS actions. The CP collects the results and detects that the VoIP server parameter is not configured properly with the latest parameter values. CP will then reconfigure the necessary VoIP

settings on the phone using UPnP DM CMS actions. Then CP will re-run the tests, then collect the results again and inform Maria via the GUI that the phone is reconfigured and tests have been successfully passed. Maria can now enjoy her VoIP service with her new phone.

- Tony owns an LCD TV, but it has picture problems. After contacting manufacturer support, Tony must exchange his defected TV for the same model. However he does not want to reconfigure all the settings again. Using a manufacturer Control Point installed on his computer, he is able to make a backup of all settings and store it on his PC using UPnP DM CMS actions. Once the new TV is delivered, he is able to restore the configuration with the Control Point so that the new TV is rapidly setup with all his favorite settings.

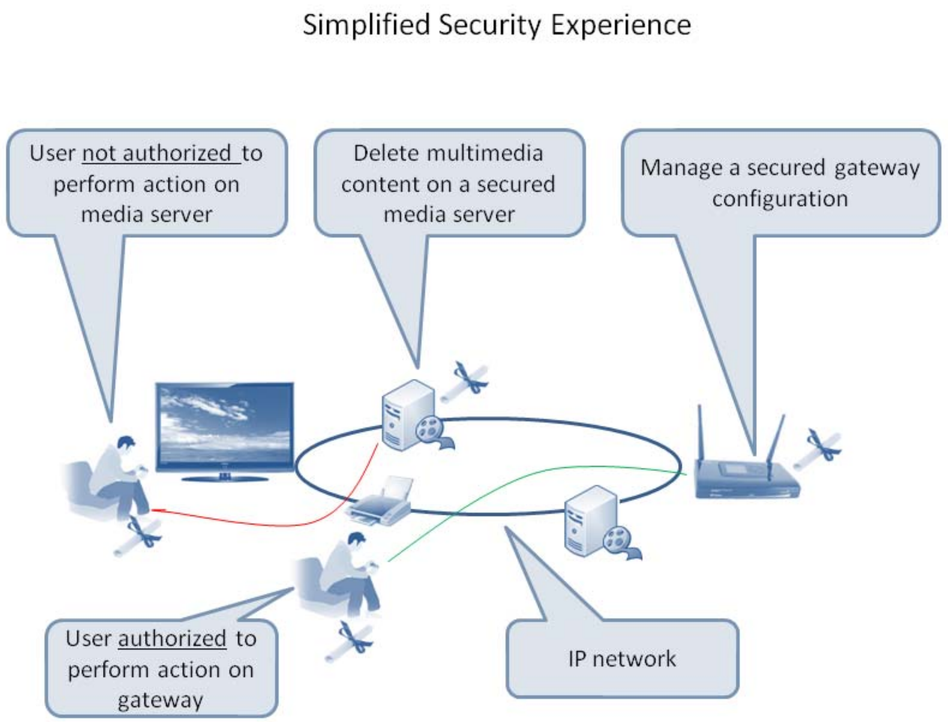
SECURITY

As UPnP DM provides sensitive management operations, it is critical for users, manufacturers and service providers to ensure that control points (and their users) will have the appropriate level of authorization to access management actions. In addition some actions will have to use a secured communication channel.

This will prevent

- Malicious control points from trying to manage a device and device services.
- Malicious devices/applications from intercepting device management operations (known as "man in the middle").
- Malicious application (installed using UPnP DM) from attacking the device.

UPnP Device Management version 2 will focus on providing necessary security features. It will require the presence of UPnP Device Protection:1 [DPS] in order to prevent any Control Point to run any action on any device. UPnP Device Protection has been published in March 2011 by the UPnP Forum (more information on this DCP can be obtained from http://upnp.org/specs/gw/deviceprotection1).


Simplified Security Experience
User not authorized to perform action on media server
Delete multimedia content on a secured media server
Manage a secured gateway configuration
User authorized to perform action on gateway
IP network

A secured device may only allow authenticated Control Points to invoke some sensitive actions and access protected sections of its data model.

Such security features allow implementers to decide for instance which part of the manageable device data model will be visible and under which conditions. In fact UPnP DM version 2 will specify a security model that allows manufacturers and service providers to define their own level of security for their services or devices.

CONCLUSION

UPnP Device Management provides operations and data models to be able to maintain, troubleshoot, configure and manage software and to enable services on UPnP-enabled IP devices.

This management protocol brings value for different stakeholders:

- Users, by simplifying the management of the electronic connected devices and possibly sharing a centralized solution to manage all its home IP devices.
- Manufacturers and Service Providers, by standardizing the device maintenance so they can provide a unique solution for customer that can also be remotely accessed through remote management proxies for customer support.

The adoption of UPnP DM standard can therefore lead to the following benefits:

- A technical solution for adding management functionalities on retail devices, which are also supporting the standards DLNA, DVB and Open IPTV Forum.
- A technical solution for adding local management functionalities of Home Gateways (in accordance with the HGI requirements and BBF specifications) that add more flexibility to the mechanisms currently provided by the UPnP IGD.
- A technical solution allowing the deployment of a proxy between the remote management of Home Gateway (e.g. provided by CWMP) and the UPnP devices in the home network and supporting data model mapping between protocols.

UPnP Device Management version 1 is available for implementers since July 2010 at http://upnp.org/specs/dm/dm1.

UPnP Device Management version 2 will focus on adding security to UPnP Device Management and will also provide bandwidth test and alarm management. It is planned to be released in Q3 2011.

JOIN UPnP FORUM

UPnP Forum is open to any company interested in making home or office networking easy for users. UPnP Forum seeks to facilitate seamless connectivity of devices and simplify network implementation in home and small business environments. Toward this end, UPnP Forum Members work together to define and publish Device Control Protocols (DCPs) built upon open, Internet-based communications standards. UPnP Forum offers two levels of membership—basic and implementer, catering to a variety of member needs.

Basic Membership offers the following opportunities with no annual fee:

- **Leadership.** Design and drive the device descriptions for your industry's products and services and the products with which they will interact.
- **Leverage your assets.** Ensure that your legacy products and new products can talk and interact dynamically on UPnP network.
- **Learn more.** Gain a broad understanding of UPnP Forum technology and its opportunities for your products and industry.
- **Leverage Forum market development.** Gain access to UPnP Forum events including Plugfest compatibility workshops, UPnP Forum Partner Pavilions at major trade shows, use of the UPnP Forum Member logo, and public relations support.
- **Find partners.** Interact with and leverage the resources of the large, diverse group of organizations actively creating and investing in UPnP Forum technology.

UPnP Forum certification process is open to vendors who are Implementer level members of UPnP Forum and have devices that support UPnP Forum technology. The annual fee for implementer membership in UPnP Forum is US $5,000.

Implementer Members enjoy all the benefits of Basic Members and the following additional benefits:

- Access to the official UPnP Certification test tool and ability to test devices for UPnP® Certification.
- Special assistance in obtaining technical support from the test tool product support team.
- License to the UPnP® Certification Mark for display on certified products and associated product marketing collateral.
- Ability to include the member company’s certified devices in the online listing of certified devices.

Steering Committee Members provides UPnP Forum leadership and business direction, while delegating to several technical working committees to identify and define UPnP services, device controls and protocols (DCPs) and usage scenarios. Membership to the Steering Committee is by election which is open to any Implement Member. Currently, the UPnP Forum Steering Committee is composed of representatives from the following companies:

Alcatel·Lucent	CableLabs®	intel®
LG	NOKIA	orange™
PHILIPS	SAMSUNG	SONY

For more information about joining UPnP Forum or about certifying your product, visit: http://www.upnp.org. Send questions of an administrative nature to UPnP Forum upnpadmin@forum.upnp.org with the text *"UPnP Administration Request"* in the subject line of your message.

Contact

Dr. Alan Messer
President and Chairman
UPnP Forum
upnpadmin@forum.upnp.org
+1 503-619-5223

UPnP℠
FORUM