ISO/IEC 29341-8-5

Edition 1.0 2008-11

INTERNATIONAL STANDARD

Information technology – UPnP Device Architecture – Part 8-5: Internet Gateway Device Control Protocol – Wireless Local Area Network Access Point Device

ISO/IEC 29341-8-5:2008(E)

About the IEC

About IEC publications

ISO/IEC 29341-8-5

Edition 1.0 2008-11

INTERNATIONAL STANDARD

Information technology – UPnP Device Architecture – Part 8-5: Internet Gateway Device Control Protocol – Wireless Local Area Network Access Point Device

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE F

ICS 35.200

ISBN 2-8318-1009-6

CONTENTS

LIST OF TABLES

INFORMATION TECHNOLOGY –
UPNP DEVICE ARCHITECTURE –

Part 8-5: Internet Gateway Device Control Protocol – Wireless Local Area Network Access Point Device

FOREWORD

1) ISO (International Organization for Standardization) and IEC (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. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

7) All users should ensure that they have the latest edition of this publication.

8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

9) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

IEC and ISO 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 the putative patent rights. The holders of the putative patent rights have assured IEC and ISO that they are willing to negotiate free licences or licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of the putative patent rights are registered with IEC and ISO.

Intel Corporation has informed IEC and ISO 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 IEC and ISO 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 IEC and ISO 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 IEC and ISO 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 IEC and ISO 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 IEC and ISO 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 IEC and ISO 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. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29341-8-5 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.

The list of all currently available parts of the ISO/IEC 29341 series, under the general title *Universal plug and play (UPnP) architecture*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

ORIGINAL UPNP DOCUMENTS (informative)

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 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 Document Title	ISO/IEC 29341 Part
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

1. Overview and Scope

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

This document defines the REQUIRED **ROOT** device
urn:schemas-upnp-org:device:*WLANAccessPointDevice*.

The ***WLANAccessPointDevice*** encapsulates services for the Access Point Device Control Protocol (DCP).

The Wireless LAN (WLAN) Access Point (AP) is a device that implements the IEEE 802.11 (a, b, g) wireless standards to provide an 'infrastructure' network for home or small business. The device definition does not include access point usage in 'hotspots' or enterprise networks.

The AP acts as an Ethernet bridge that enables attachment of multiple nodes to a LAN. Figure 1a shows a common topology used for a network with WLAN access point. Figure 1b shows use of access point as a way to extend the reach of a local area network. The DCP covers both the cases.

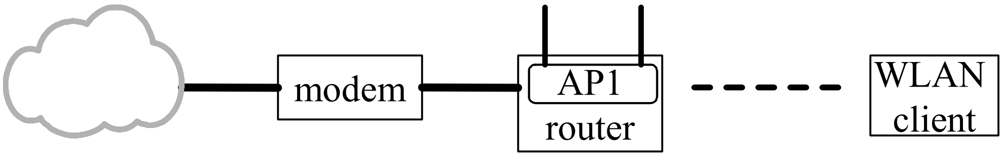

Figure 1a: *WLANAccessPointDevice* – common usage model

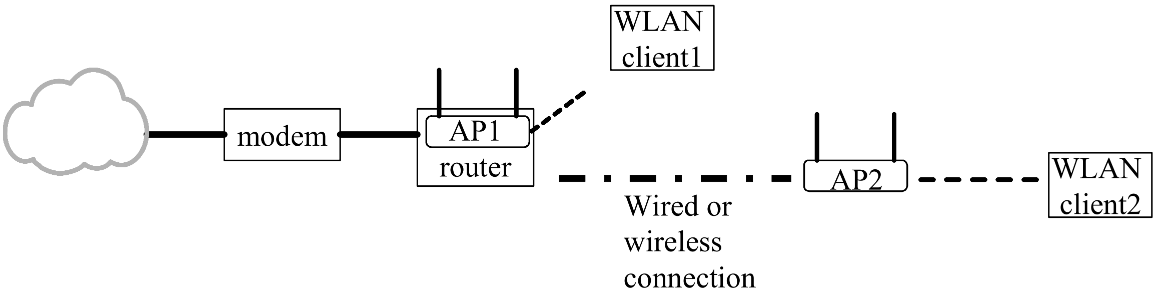

Figure 1b: Extending an existing network – example topology

1.1. Focus and Goals for DCP version 1.0

The Internet Gateway Device (IGD) Working Committee agreed to focus on the following set of functionalities in coming up with the services for AP DCP v1.0.

- Configuring and querying 802.11 access point parameters.
- Bootstrapping of link security for WLANs that use 802.11based access points. This includes secure introduction of the wireless client and the AP device. The goal is to make it easier to setup and configure WLAN security for 802.11 access points and manage WLAN access authorization.

1.2. Non-Goals for DCP version 1.0

The following work items were briefly discussed and considered to be beyond the scope of this version of the DCP.

- Replacing or enhancing the link security mechanism provided by the access point.
- Configuration services for access point for 'hotspot' and enterprise networks

1.3. WLAN Security Requirements and Recommendations

Link security is critical for wireless home network because connectivity is not restricted by the reach of wires or availability of physical ports. The likelihood of unintentional cross-links and malicious drive-by attacks is bound to increase along with the popularity of WLANs. This will be detrimental to the user experience with wireless networks and will impede introduction of new product categories and usage models. Consumers and service providers will demand link security as part of the WLAN package.

An alternative to link security is to protect specific resources with security mechanisms involving higher (network or application) layers of the networking software stack. However, it cannot be expected of the average home user to be technically savvy and to take the trouble to identify all the vulnerable points (data/devices) in the home network for protecting them individually with appropriate methods.

Currently the most common way to secure 802.11 links in the home involves Wired-Equivalent Privacy (WEP) based encryption and authentication. The security risks when using WEP are well known. An attacker can crack the WEP key by collecting packets with a wireless 'packet sniffer' and running widely available utilities to determine the WEP key. If the WLAN owner becomes aware of the security compromise, the WEP key on all the clients and AP has to be updated, since the same WEP key is used for all nodes.

In order to build consumer confidence and expand usage of wireless applications, it is important for the home WLAN devices to adopt stronger security mechanisms such as Wireless Protected Access (WPA) currently being proposed in the 802.11 industry. Longer term, it is expected that the security specification being worked on in the 802.11i working group would be the widely adopted and appropriate solution for a strong security mechanism on the AP. The security enhancements provide per-user based authentication, per-session keys, frequent re-keying and stronger encryption methods such as Advanced Encryption Standard (AES).

One of the main issues with the use of security in WLAN is the process of setting up the security parameters. Current mechanisms used for initializing link security on an AP device are not very user-friendly. For example, with the WEP-based model, the user has to retrieve a long WEP key for the AP either through a secure/wired connection first and enter it on the new client correctly. This problem of bootstrapping also exists with the mechanisms proposed as an improvement on the plain WEP-based security. Because of this, users are likely to not enable security in their network, leading to several vulnerabilities. The objective of the 802.11 security initialization mechanism using UPnP technology as proposed in this document is to reduce user involvement and introduce an intuitive usage model for users to take advantage of the higher level of security the access points can offer.

An overall security solution should protect the user from 'man-in-the-middle' attacks by preventing the user's client from associating with an unfriendly AP and the user's AP from associating with a foreign client. It should prevent session-hijack attacks by making sure all messages between the AP and client are authenticated. It should not be prone to dictionary attack, e.g., attacker deciphering the password after sniffing challenge and response exchange from a password-based protocol.

The objective of the DCP is to enable a secure WLAN solution with AP devices that implement the required elements specified in the DCP. The following figure shows the major functional components of the WLANAccessPointDevice.

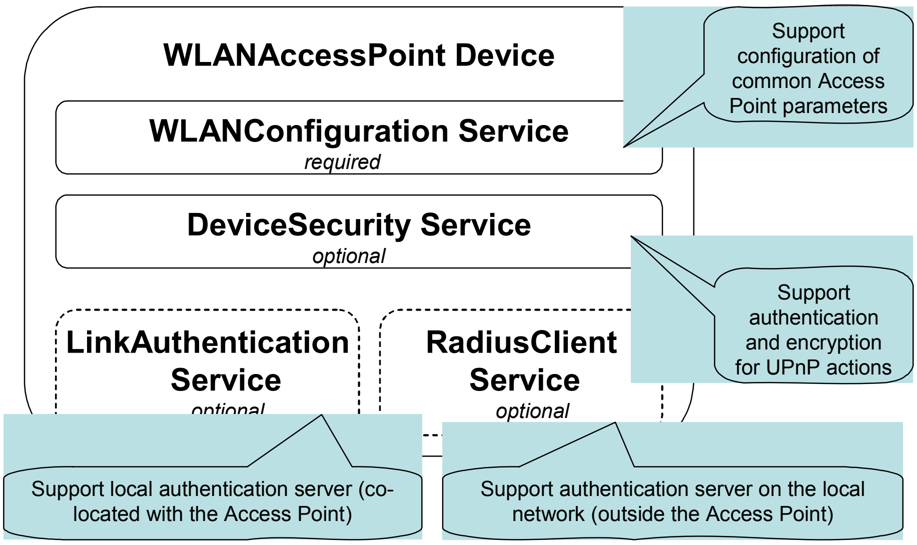
WLANAccessPoint Device
WLANConfiguration Service
required
DeviceSecurity Service
optional
LinkAuthentication Service
optional
RadiusClient Service
optional
Support configuration of common Access Point parameters
Support authentication and encryption for UPnP actions
Support local authentication server (co-located with the Access Point)
Support authentication server on the local network (outside the Access Point)

Figure 2: ***Functional components of WLANAccessPointDevice***

1.3.1. AP Parameter Configuration

The *WLANConfiguration* service, a required service of *WLANAccessPointDevice,* provides state variables for some of the access point parameters that were identified by the working group to be useful to be configured via a UPnP client. They provide the ability to easily configure security and operation parameters, offer diagnostic information and help set up repeater functionality. In addition, UPnP technology also provides event notification capability to inform interested clients on the status of the AP. With an AP that is not enabled with UPnP technology, users may have access to some of these parameters via a Web browser with no strong mechanism for authentication and access control. Also, the configuration actions sent between that AP and client are not protected for confidentiality and are vulnerable to attack.

It is highly recommended for the AP DCP to have a mechanism to authenticate access to the UPnP actions, and provide confidentiality of the data. It is also recommended to have a mechanism to exclude unauthenticated and non-confidential access to the parameters that can only be accessed through secure UPnP actions. Without such access control any client device in the LAN can change the configuration of the AP, affecting the whole network. A client that has access to the secure link cannot necessarily be trusted with the administration capability. This situation is especially relevant in a small business environment. Restricting write access to the AP parameters will lessen the support burden on network equipment vendors and service providers.

It is recommended to use the actions defined in *DeviceSecurity* service to implement access control. The working group has identified specific actions in the *WLANConfiguration*, *LinkAuthentication* and *RadiusClient* service that are recommended to be secure.

1.3.2. Support for per-client credentials

The AP *MAY* have the capability to support authentication of individual WLAN clients with unique credentials. It *MAY* do this without an authentication server by using multiple PSK WPA keys. Or, the AP *MAY* do this by having a pointer to an authentication server such as a RADIUS server that is external to the AP device via variables provided in the *RadiusClient* service. Alternatively, the AP *MAY* support a co-located authentication server functionality and provide it as a UPnP service, specifically the *LinkAuthentication* service. This is an optional service that can be used with the AP DCP to support per-client authentication with a co-located authentication server.

Please refer to the *LinkAuthentication* and *RadiusClient* service definition documents for more details.

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**:*WLANAccessPointDevice:1*

2.2. Device Model

It is recommended that *WLANAccessPointDevice* 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 *WLANAccessPointDevice* implementation OR in a device that encompasses the *WLANAccessPointDevice*. These two models are described below.

2.2.1. Description of Device Requirements

The following table briefly describes the purpose of the services used in *WLANAccessPointDevice*.

Service Name	Service Description
WLANConfiguration	Configuration parameters associated with a WLAN link that needs to be accessed programmatically.
DeviceSecurity	Actions for taking ownership, configuring access control, establishing secure sessions, and invoking secure actions.

2.2.1.1. DeviceSecurity within WLANAccessPointDevice

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

Table 1: Device Requirements for stand-alone *WLANAccessPointDevice*

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
			WLANConfiguration:1	*R*	*WLANConfiguration1*
			DeviceSecurity:1	*O*	*DeviceSecurity1*
			Non-standard services embedded by an UPnP™ device vendor go here.	*X*	*TBD*

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

Relationship between Services

Figure 3 shows the logical structure of the device and services defined by the working group for UPnP technology enabled APs.

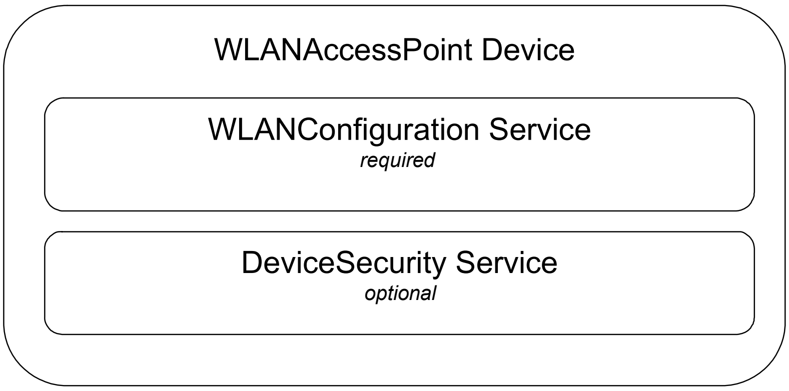

Figure 3: *DeviceSecurity* within *WLANAccessPointDevice*

In addition, the *LinkAuthentication* service (optional) may be used if an AP supports per-client authentication with a co-located authentication server. *LinkAuthentication, RadiusClient,* and *WLANConfiguration* services may be dependent on the *DeviceSecurity* service for providing access control to the actions defined in the services.

2.2.1.2. DeviceSecurity outside WLANAccessPointDevice

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

Table 2: Device Requirements for embedded *WLANAccessPointDevice*

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
			WLANConfiguration:1	*R*	*WLANConfiguration1*
			Non-standard services embedded by an UPnP™ device vendor go here.	*X*	*TBD*

[1] R = Required, O = Optional, X = Non-standard. .

[2] Prefixed by urn:**upnp-org**:**serviceId**: .

Relationships between Services

Figure 4 shows the logical structure of the device and services defined by the working group for UPnP technology enabled APs that may use the DeviceSecurity service for other UPnP devices contained in the same physical device. In addition, the optional *LinkAuthentication* service may be used if an AP supports per-client authentication with a co-located authentication server. *LinkAuthentication, RadiusClient,* and *WLANConfiguration* services may be dependent on the *DeviceSecurity* service for providing access control to the actions define in the services.

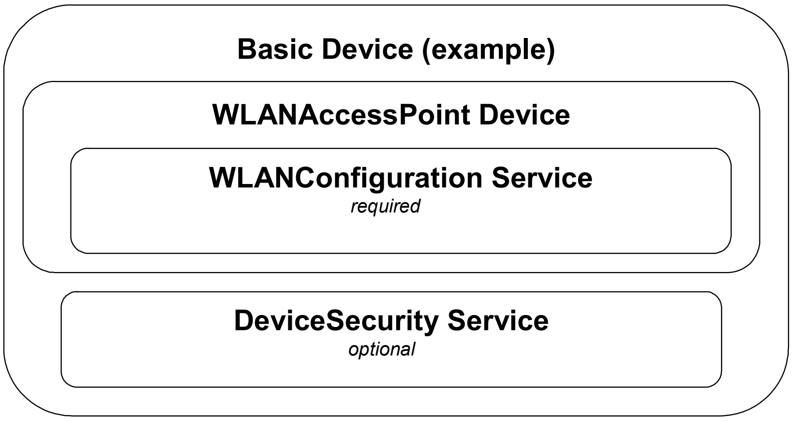

Figure 4: Example of *DeviceSecurity* outside *WLANAccessPointDevice*

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 *WLANAccessPointDevice*.

2.3. Theory of Operation

This section describes the general usage model of the services defined in the AP device. This section starts by listing the requirements and optional features of the WLAN nodes. This is followed by a section describing the various scenarios reflecting the use of these features. For each of these, the benefits enabled by the UPnP services are explicitly highlighted.
It is highly recommended for the AP DCP to use DeviceSecurity service to secure specific UPnP AP actions. This section assumes an overall understanding of UPnP Security concepts. Please refer to the *DeviceSecurity:1* Service Control Specification defined by UPnP Security WC for a more detailed description of the theory of operation of a secure UPnP device.

2.3.1. WLAN node Requirements

From the perspective of requirements, a WLAN node falls into one of two categories – the access point and the wireless client (station) of the access point.

2.3.1.1. AP Requirements

The 802.11 access point requirements are listed below along with some optional features.

- The AP *MUST* be addressable via the Internet Protocol (IP) protocol using both the wired and wireless interfaces. The AP functionality *may* be co-located with router/'UPnP Internet Gateway Device' (IGD) functionality and/or a modem for Internet access.
- The AP *MUST* provide a user the ability to physically reset it to factory default settings.
- The AP *MUST* support Wireless Protected Access (WPA) in pre-shared key (PSK) mode. It *MUST* support at least 10 PSKs.
- The AP *MAY* implement *DeviceSecurity* service as defined in the *SecureDevice* Device Control Protocol v1.0. This involves use of a public-private key pair and a cryptographic library for authentication and encryption.
- The AP *MAY* support 802.1x via a RADIUS client (RFC2865, IETF) using *RadiusClient* UPnP service.
- The AP *MAY* support 802.1x via *LinkAuthentication* service

It is not required of the AP to have link security ON by default.

2.3.1.2. Client requirements for AP Configuration

If configuration of AP parameters is desired, there *MUST* be at least one client in the LAN that has an interactive user interface. Other WLAN clients *MAY* be UPnP technology enabled and be able to execute UPnP Control

Point functionality to send UPnP actions to the AP. All wireless clients are required to have the same link security mechanism that is used by the AP (e.g., 802.1x). The WLAN client must at least support WEP.

2.3.2. Scenarios for introduction of WLAN clients to the AP

In addition to easy configurability of AP parameters that are detailed in the *WLANConfiguration* service, the AP DCP also provides a common framework for credential provisioning with sufficient room for vendor differentiation. The following sections describe the different scenarios involved when a WLAN client comes in contact with the AP for the first time and the role of UPnP technology.

2.3.3. Setting up a secure control point (if DeviceSecurity is implemented in AP device)

WLANConfiguration service provides a set of actions to modify and query a set of parameters on the 802.11 access point. The actions in this service that modify parameters should be authenticated via UPnP security. 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.

Upon powering up the AP, the user would run the ‘AP application’ (control point) on a client to take ownership of the AP as per UPnP Security protocol. Refer to the *DeviceSecurity:1* Service Control Specification defined by UPnP Security WC for details on *TakeOwnership* function. By ‘taking ownership’ this client would have the authority to allow specific control points to configure the AP e.g., enter security parameters, turn security on, switch to repeater mode etc.

Note that in the event that the Security Console application was not available to begin with, the AP would continue to function in the default mode, with no configuration possible via UPnP technology.

2.3.4. AP uses network-wide credentials for authentication

The AP uses pre-shared network-wide credential as specified in WPA for all clients or uses WEP-only based authentication.

2.3.4.1. Initial configuration of the AP

The ‘AP application’ configures the shared key(s) in the AP, and enables WEP or WPA security. Note that if the ‘AP application’ is a WLAN client, it has to re-establish the link to the AP once link security has been enabled, using the new key.

Benefits *and assumptions* of using UPnP technology:
UPnP technology provides easy discovery and configuration of the AP device via a standardized programmatic interface. With an AP that is not enabled with UPnP technology, the user has to enter the URL for the AP’s web server and type in the shared key. The shared key would have to be very long to be sufficiently secure, especially since it can be used anytime to access the AP’s web server. In addition, the user has to be aware of the WEP or WPA key and enter it through the browser.

2.3.4.2. Enrollment of subsequent clients

If the AP is using WPA PSK or WEP for network-wide authentication, there is no per-client authentication and therefore no need for *LinkAuthentication* service, *RadiusClient* service or any authentication server such as RADIUS on the WLAN. If the client device has a UI, the user enters the shared key (WEP or WPA PSK) and gets link access to the AP. If the client device does not have a UI, it should be pre-programmed with a unique key that is made available to the user, e.g., via a label on the chassis. The user will enter this shared key into the AP using a Control Point application. The number of such devices that can be added is limited to the number of shared keys supported by the AP device. In the case of WEP this will be four, and with WPA PSK this will be a minimum of ten.

An alternate mechanism for UPnP technology enabled clients is for the client device to be directly connected (e.g., Ethernet cable) to the AP. The client runs a UPnP control point and retrieves the shared key, configures itself and is ready to connect to the WLAN.

Benefits *and assumptions* of using UPnP technology:
Easy mechanism for adding new clients without UI to an AP that supports network wide shared keys. The alternate mechanism mentioned above provides a way to do this without the user having to enter keys, *assuming that the client implements UPnP™ Control Point functionality, and that the clients provide a wired interface for enrollment in addition to the wireless capability.* With an AP that is not enabled with UPnP technology, the WLAN clients do not have a common mechanism to access the security parameters of the AP.

2.3.5. AP uses client-specific credential for authentication

If the AP implements an authentication mechanism (e.g., 802.1x) that uses different authentication credentials for each client, an authentication database is used to store and update these credentials. The authentication database may or may not be co-resident with the AP. If it is maintained within the AP device, the *LinkAuthentication* service would provide an interface to this database. The *LinkAuthentication* service provides actions for enabling a new client to be enrolled into the secure WLAN. This database is consulted by the AP's authentication system for validating a client that wants to establish link security with the AP. If the AP uses an external authentication server such as a RADIUS server, the AP should be configured with the addresses, ports and secrets to access these servers using the actions provided in the *RadiusClient* service.

2.3.5.1. Initial configuration of the AP

If the AP uses an external authentication server, the control point application sets information about authentication servers (such as IP addresses, port, etc.) in the *RadiusClient* service via UPnP technology. An entry corresponding to this client will have to be added to the external authentication server (out of band) before enabling link security. If a co-located authentication server is used, depending on the control point implementation, it may make an entry corresponding to this client along with its credential in the *LinkAuthentication* service via UPnP technology.

Benefits *and assumptions* of using UPnP technology:
A WLAN client is enabled for programmatic configuration of the wireless interface of the AP (including enabling of link security on AP), *assuming that the client implements UPnP™ Control Point functionality, the client does not need a wired interface in addition to the wireless interface.* With an AP that is not enabled with UPnP technology, there is no easy method to add an entry for the first client or authentication related parameters into the AP.

2.3.5.2. Enrolling subsequent clients

If the AP supports a co-located authentication server, the UPnP Control Point application is used for enrolling new clients into the secure WLAN. The new client that attempts authentication by the AP is not required to have an interactive user interface or be UPnP technology enabled. It is assumed that this client supports the authentication method required by the AP for link security (e.g., 802.1x). The mechanism uses the optional *LinkAuthentication* service and the process of enrollment is described in the *LinkAuthentication* service document.

If the authentication server is external to the AP an out-of-band mechanism (other than UPnP technology) would be used to update the database used by this authentication server resulting in the addition of an entry corresponding to the new client.

In both cases, it is assumed that the WLAN client has the capability to authenticate the AP device during enrollment and subsequent authentication,

Benefits *and assumptions* of using UPnP technology:
In the situation where the authentication server is co-located, the use of the *LinkAuthentication* service on the AP simplifies the administration of 802.1x authentication and makes it more usable in a home environment. A new WLAN client can be enrolled into the secure WLAN using the Control Point application. The *LinkAuthentication* service provides a common interface for modifying the 802.1x authentication database.

When the authentication server is not co-located, the optional *RadiusClient* service provides the necessary variables and actions for any program to configure the AP with information about the authentication server(s). *There is an assumption that there is a client running in the network that implements UPnP™ Control Point and provides a user interface; the new WLAN client does not need a wired interface in addition to the wireless interface.*

3. XML Device Description

```
<?xml version="1.0"?>
<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:WLANAccessPointDevice: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>
      <!-- XML to declare other icons, if any, go here -->
    </iconList>
    <serviceList>
      <service>
        <serviceType>urn:schemas-upnp-
org:service:WLANConfiguration:1</serviceType>
        <serviceId>urn:upnp-org:serviceId: WLANConfiguration1</serviceId>
        <SCPDURL>URL to service description</SCPDURL>
        <controlURL>URL for control</controlURL>
        <eventSubURL>URL for eventing</eventSubURL>
      </service>
            <!-- Declarations for other services added by UPnP™ vendor (if
any) go here -->
    </serviceList>
    <deviceList>
      Description of embedded devices added by UPnP™ vendor (if any) go
here
    </deviceList>
    <presentationURL>URL for presentation</presentationURL>
  </device>
</root>
```

4. Test

No semantic tests are defined for this device.

5. Annex 1 (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 *WLANAccessPointDevice*. This is used by the Security Console to assign access control of secure actions on the AP device to control point applications. Please refer to the *DeviceSecurity1.0* service specification for more details about Security Console, Permissions, Profiles and ACLs.

5.1. Permissions

The following permission is to be defined to allow access control to the secure actions of the services embedded in the AP device. This would apply to *LinkAuthentication* and *RadiusClient* services if they are included in the AP device implementation. The permission is to be implemented in the following XML format:

```
<Permission>
        <UIname>APControl</UIname>
        <ACLEntry>
                <APWG:APDeviceAll/>
        </ACLEntry>
        <FullDescriptionURL></FullDescriptionURL>
        <ShortDescription>
                This permission allows the control point to set and get all secure actions
                of all the services of the AP device.
        </ShortDescription>
</Permission>
```

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

The above defined permission is to be returned by the AP device in the “DefinedPermissions” argument of *DeviceSecurity*’s GetDefinedPermission action. It is possible that vendors may define additional set of permissions for access control to the AP device. For example, they may provide separate *admin* and *user* permissions for further granularity of access.

If *DeviceSecurity* service resides inside the *WLANAccessPointDevice* it will contain only the defined permissions of the AP device (as mentioned above). The “DefinedPermissions” argument of GetDefinedPermission action returned by the *DeviceSecurity* would be:

```
<DefinedPermissions>
        <Permission>
                <UIname>APControl</UIname>
                <ACLEntry>
                        <APWG:APDeviceAll/>
                </ACLEntry>
                <FullDescriptionURL></FullDescriptionURL>
                <ShortDescription>
                        Allow this application to complete control of the Wireless Access Point
                device.
                </ShortDescription>
        </Permission>
</DefinedPermissions>
```

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

```
<DefinedPermissions>
    <Permission>
        <UIname>APControl</UIname>
        <ACLEntry>
            <APWG:APDeviceAll/>
        </ACLEntry>
        <FullDescriptionURL></FullDescriptionURL>
        <ShortDescription>
            Allow this application to complete control of the Wireless Access Point
        device.
        </ShortDescription>
    </Permission>
    <Permission>
        e.g., Permission defined by IGD Device
    </Permission>
…
</DefinedPermissions>
```

5.2. Profiles

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

5.3. Access Control List (ACL) entry

If DeviceSecurity service is implemented in the UPnP AP device, *WLANAccessPointDevice* would only have the "<APWG:APDeviceAll>" 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>
            <APWG:APDeviceAll/>
        </access>
        <valid>
            <not-before>2001-10-23_05:17:32</not-before>
            <not-after>2003-12-31_23:59:59</not-after>
        </valid>
    </entry>
</acl>
```

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch