WFA Device 1.0

Template Version 1.01

January 2006

Contents

List of Tables

1. Overview and Scope

This device template is compliant with the UPnP ™ Architecture, Version *1.0* as a vendor extended UPnP device.

This document defines the REQUIRED **ROOT** device
urn:schemas-wifialliance-org:device:*WFADevice*

The ***WFADevice*** encapsulates services for the WFA Device Control Protocol (DCP).

The Wi-fi Alliance (WFA) device implements IP based transports (such as Ethernet/802.3 wired standards) to provide an out-of-band mechanism to configure IEEE 802.11 (a,b,g) settings on the device so the device may authenticate and associate with a secured wireless network and on Access Points so the AP may host secure wireless networks.

1.1. Focus and Goals for DCP version 1.0

The Wi-Fi Alliance Simple Config working group has specific requirements for creating and extending wireless networks and adding wireless stations:

- Setup must be simple, a task that a typical consumer can complete
- Setup process is secure and must maximize security of the WLAN
- Consumer focus with some attention to small business cases

1.2. Non-Goals for DCP version 1.0

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

- Replacing or enhancing the link security mechanism of the WLAN
- Configuration services for access points 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 Wi-Fi Protected Access (WPA) that has become available in the market. 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 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.

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 station are authenticated.

The objective of the DCP is to enable a secure WLAN solution with combined Wi-Fi and IP connected devices that implement the required elements specified in the DCP. The following figure shows the major functional components of the WFADevice.

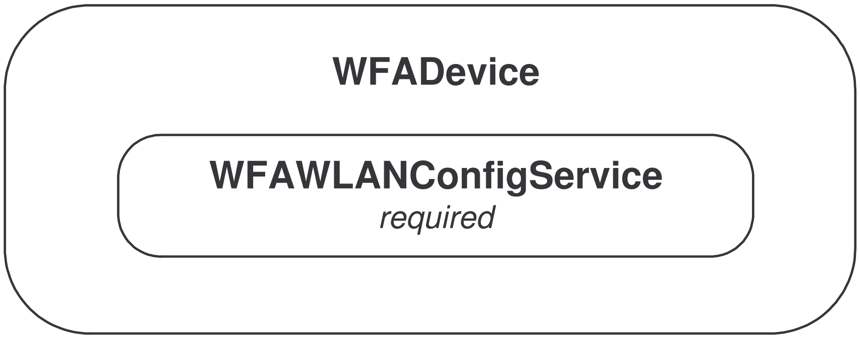

Figure 1: ***Functional components of WFADevice***

1.3.1. Station Parameter Configuration

The ***WFAWLANConfig*** service, a required service of ***WFADevice,*** provides state variables for some of the wireless station parameters. They provide the ability to easily configure security and operation parameters, and offer diagnostic information. In addition, UPnP also provides event notification capability to inform clients responsible for Wi-Fi device configuration on the status of the Wi-Fi station.

The Simple Config protocol that is imbedded in the exchange between the control point and the WFA Device perform authentication and encryption so that the UPnP actions do not require any additional security. The state variables in any WFA Device service must not return directly the binary data that is contained. If requested for a state variable action, the device may return a null or may choose to follow the Simple Config rules and encrypt the contents with an arbitrary SID or the SID of the requesting control point if known.

2. Device Definitions

2.1. Device Type

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

urn:**schemas-**wifialliance-org**:device**:*WFADevice:1*

2.2. Device Model

It is required that *WFADevice* be implemented with support for the WFA Simple Config secure association protocol.

2.2.1. Description of Device Requirements

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

Service Name	Service Description
WFAWLANConfig	Configuration parameters associated with a WLAN device that needs to be accessed programmatically.

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

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
			WFAWLANConfig:1	*R*	*WFAWLANConfig1*
			Non-standard services embedded by an UPnP vendor go here.	*X*	*TBD*

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

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

Figure 3 shows the logical structure of the device and the single service defined for UPnP enabled WLAN devices.

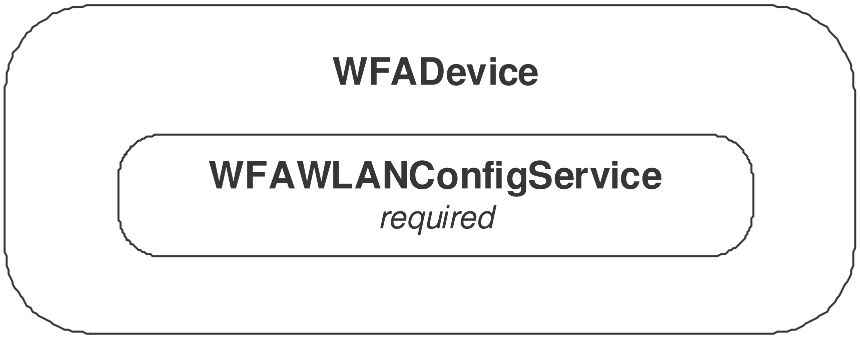

Figure 3: *WFAWLANConfig Service* within *WFADevice*

2.3. Theory of Operation

This section describes the general usage model of the services defined in the WFA interface 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.

2.3.1. WLAN node Requirements

From the perspective of requirements, a WFADevice is a WLAN node that also has an Ethernet or other established IP interface for, at a minimum, the purpose of discovering the device and configuring the WLAN settings of the device.

The WLAN node requirements are listed below:

- The device *MUST* be addressable via the Internet Protocol (IP) protocol using the Ethernet interface.
- The device *MUST* provide a user the ability to physically reset it to factory default settings.
- The device *MUST* implement the *WFA Simple Config protocol*. This involves use of a predefined password (typically a PIN) and a public-private key pair and a cryptographic library for encryption and authentication.
- The device *MAY* implement the *Proxy Function* as defined in the *WFAWLANConfigService v1.0* specification. This service allows for any WLAN station to send an event when a new WLAN Enrollee is requesting WLAN configuration.

2.3.1.1. Client requirements for Configuration of WLAN Parameters

If configuration of WLAN parameters over the UPnP/IP channel is desired, there should be at least one client in the LAN that has an interactive user interface. Other WLAN clients *MAY* be UPnP enabled or not, and they may be able to execute UPnP Control Point functionality to send UPnP actions to the WLAN station.

2.3.2. Configuration of New Clients to the WLAN

WFAWLANConfig service provides a set of actions to query and modify a set of 802.11 parameters on the WLAN client over an IP interface. Acquisition of the WLAN settings by the Registrar performing configuration is performed in several ways:

- using the actions defined in the WFAWLANConfigService v1.0 or associated vendor extensions.
- From a local store on the Registrar, possibly from a previous wireless client configuration for networks that use a single PSK.
- Current wireless settings of the Registrar (for a WLAN attached device).
- Input from the user.

The PSK is encrypted using the public key based protocol specified the WFA Simple Config specification. Settings are sent using the action specified in the WFAWLANConfig service. The data sets are validated and the settings are encrypted using the WFA Simple Config exchange mechansim.

The WFA device attempts to associate with the WLAN and reports state.

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-wifialliance-org:device:WFADevice: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-wifialliance-
org:service:WFAWLANConfig:1</serviceType>
        <serviceId>urn: wifialliance-org:serviceId:WFAWLANConfig1</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.