USER GUIDE

WLAN Module

WMG623A

USER GUIDE

WMG623A

WLAN Module

WMG623A
E042010-CS-R01
XXXXXXXXXXXXX

COMPLIANCES

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC RADIATION EXPOSURE STATEMENT

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

THIS DEVICE IS INTENDED ONLY FOR OEM INTEGRATORS UNDER THE FOLLOWING CONDITIONS:

1. The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2. The transmitter module may not be co-located with any other transmitter or antenna.

3. For all products marketed in the US, OEM has to limit the operation channels in CH1 to CH11 for 2.4 GHz band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as the three conditions above are met, further transmitter tests will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions cannot be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

END PRODUCT LABELING

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: “Contains FCC ID: V8YFIXHI623A000W”.

MANUAL INFORMATION TO THE END USER

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/ warning as show in this manual.

ABOUT THIS GUIDE

PURPOSE This guide details the hardware features of the WMG623A WLAN Module, including its physical and performance-related characteristics, and how to install the device and use its configuration software.

AUDIENCE This guide is for PC users with a working knowledge of computers. You should be familiar with Windows operating system concepts.

CONVENTIONS The following conventions are used throughout this guide to show information:

NOTE: Emphasizes important information or calls your attention to related features or instructions.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

WARNING: Alerts you to a potential hazard that could cause personal injury.

RELATED PUBLICATIONS The following publication gives basic information on how to install and use the WMG623A WLAN Module.

Quick Installation Guide

REVISION HISTORY This section summarizes the changes in each revision of this guide.

APRIL 2010 REVISION
This is the first revision of this guide.

Contents

1 INTRODUCTION

The WMG623A is a Wi-Fi PCI Express Card that allows simple design-in 802.11b/g/n Wi-Fi functionality for various products, such as notebooks and home gateways.

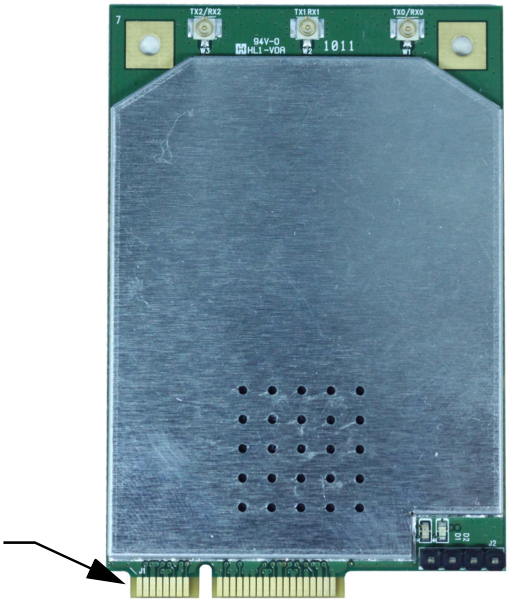
The WMG623A includes a built-in high-performance CPU that off-loads Wi-Fi packet processing tasks from the main processor. The hardware form factor follows the PCI Express standard, but the data path conforms to an RGMII interface. The result is a card that delivers a higher data transmit rate than conventional mini-PCI modules.

The WMG623A is compliant with IEEE 802.11n standard and operates in the 2.4 GHz frequency band. The card's MIMO antenna architecture is 2T3R (two transmit, three receive), which supports up to 450 Mbps throughput rate. The card also supports 20 MHz and 40 MHz bandwidth channels, as specified in the 802.11n standard.

WMG623A HARDWARE DESCRIPTION

The figure below shows the WMG623A WLAN Module.

Figure 1: The WMG623A



PCI Express Card Connector

A Hardware Specifications

Physical Specifications

Host Interface	PCI Express Card standard, 3.3 VDC
Power Consumption	2 W maximum
Physical Size	72 x 48 mm (2.83 x 1.89 in)
Weight	17 g (0.6 oz)
Temperature	Operating: 0 to 50 °C (32 to 122 °F) Storage: -20 to 70 °C (-4 to 158 °F)
Humidity	5% to 95% (non-condensing)

Wi-Fi Specifications

Frequency range	FCC/IC/NCC: 2412 MHz ~ 2462 MHz CE, AS/NZS: 2412 MHz ~ 2472 MHz
Modulation Type	CCK, DQPSK, DBPSK for DSSS 64QAM, 16QAM, QPSK, BPSK for OFDM
Data Rate	802.11b: 11, 5.5, 2, 1 Mbps 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11n (20 MHz, 800 ns GI): 195, 175.5, 156, 130, 117, 104, 78, 65, 58.5, 52, 39, 26, 19.5, 13, 6.5 Mbps 802.11n (40 MHz, 800 ns GI): 405, 364.5, 324, 270, 243, 216, 162, 135, 121.5, 108, 81, 54, 40.5, 27, 13.5 Mbps

802.11n (20 MHz, 400ns GI): 216.7, 195, 173.3, 144.4, 130, 115.6, 86.7, 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2 Mbps

802.11n (40 MHz, 400ns GI): 450, 405, 360, 300, 270, 240, 180, 150, 135, 120, 90, 60, 45, 30, 15 Mbps

RF OUTPUT POWER 11b mode: 20 +/- 0.5 dBm (peak)
11g mode: 23 +/- 0.5 dBm (peak)
11n mode, HT20: 22 +/- 0.5 dBm (peak)
11n mode, HT40: 22 +/- 0.5 dBm (peak)

RADIO FCC Part 15C (Section 15.247)
EN 301 489-1 V1.8.1 (2008-04)
EN 301 489-17 V1.3.2 (2008-04)
LP0002
RSS-210
AS/NZS 4268

COMPLIANCES

EMC FCC Part 15B

SAR FCC IEEE C95.1

Glossary

10BASE-T IEEE 802.3-2005 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX IEEE 802.3-2005 specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

1000BASE-T IEEE 802.3ab specification for 1000 Mbps Gigabit Ethernet over four pairs of Category 5 or better UTP cable.

Access Point An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

AES Advanced Encryption Standard: An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Beacon A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key Broadcast keys are sent to stations using dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

DHCP Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption Data passing between the access point and clients can use encryption to protect from interception and evesdropping.

Ethernet A popular local area data communications network, which accepts transmission from computers and terminals.

FTP File Transfer Protocol: A TCP/IP protocol used for file transfer.

HTTP Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.11b A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

Infrastructure An integrated wireless and wired LAN is called an infrastructure configuration.

LAN Local Area Network: A group of interconnected computers and support devices.

MAC Address The physical layer address used to uniquely identify network nodes.

NTP Network Time Protocol: NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open System A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

ODFM Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

SSID Service Set Identifier: An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

SESSION KEY Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

SHARED KEY A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

SNTP Simple Network Time Protocol: SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

TKIP Temporal Key Integrity Protocol: A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

TFTP Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

VAP Virtual Access Point: Virtual AP technology multiplies the number of Access Points present within the RF footprint of a single physical access device. With Virtual AP technology, WLAN users within the device.s footprint can associate with what appears to be different access points and their associated network services. All the services are delivered using a single radio channel, enabling Virtual AP technology to optimize the use of limited WLAN radio spectrum.

WI-FI PROTECTED ACCESS WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

WEP Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA-PSK WPA Pre-shared Key: WPA-PSK can be used for small office networks with a limited number of users that may not need a high level of security. WPA-PSK provides a simple security implementation that uses just a pre-shared password for network access.