



Achieving a FIPS Compliant Wireless Infrastructure with Intel® Wireless Products

Solution Brief



Legal Disclaimer

This document is provided "as is" with no warranties whatsoever, including any warranty of merchantability, non-infringement fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification or sample

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel does not control or audit the design or implementation of 3rd party benchmarks or websites referenced in this document. Intel encourages all of its customers to visit the referenced websites or others where similar performance benchmarks are reported and confirm whether the referenced benchmarks are accurate and reflect performance of systems available for purchase.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel PRO/Wireless 3845ABG Network Connection, Intel WiFi Link 1000, Intel WiFi Link 5100, Intel WiFi Link 5300, Intel WiMAX/WiFi Link 5350, Intel Centrino Wireless-N 1000, Intel Centrino Advanced-N 6200, Intel Centrino Ultimate-N 6300, Intel Centrino Advanced-N + WiMAX 6250 and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Actual measurement results may vary depending on the specific hardware and software configuration of the computer system measured, the characteristics of those computer components not under direct measurement, variation in processor manufacturing processes, the benchmark utilized, the specific ambient conditions under which the measurement is taken, and other factors.

All plans, features and dates are preliminary and subject to change without notice.

* Third-party brands and names are the property of their respective owners.

Copyright © Intel Corporation 2010



Contents

1	Introduction	2
2	What is FIPS?	2
2.1	Validated FIPS Modules	2
3	FIPS Validated Intel Wireless Adapters	3
3.1	Supported Operating Systems.....	3
3.2	FIPS Compliant Intel Wireless Products	3
3.3	Additional Intel Wireless Product Security	4
4	Third-Party FIPS Client Software for Microsoft Windows XP	4
4.1	3eTi	4
4.2	Cisco.....	5
5	Conclusion.....	5



1 Introduction

This document presents an overview of the Intel wireless product compliance with the Federal Information Processing Standard (FIPS), which is often required by U.S. Federal, state and local governments for products that implement security.

2 What is FIPS?

The Federal Information Processing Standard (FIPS) 140 is a U.S. government computer security standard used to accredit cryptographic modules. FIPS 140 coordinates the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government. FIPS 140-1 became a mandatory standard for the protection of sensitive data in 1994 and was superseded by FIPS 140-2 in 2001. The current version of the standard is FIPS-140-2.

Federal agencies, and state and local governments rely on cryptography to secure communications and protect information used in critical infrastructures, electronic commerce and other applications. Private sector organizations wanting to do business with the U.S. Federal Government must use FIPS validated network infrastructures and wireless clients to enable more secure use and communication for mobile devices and notebook computers utilizing Wi-Fi Alliance WPA2*/IEEE 802.11i* security. Because of the robust security offered by FIPS-compliance, companies in financial services, healthcare, education and manufacturing are also incorporating FIPS into their wireless network infrastructures.

At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render the product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

2.1 Validated FIPS Modules

The National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules for the FIPS 140 Security Requirements for Cryptographic Modules and other FIPS cryptography-based standards for protection of sensitive, unclassified data of the U.S. Government. FIPS also provides guidelines governing the design, implementation and deployment of these functions.

The FIPS 140-1 and FIPS 140-2 validation certificates specify the exact module name, hardware, software, firmware, and/or applet version numbers. The cryptographic libraries are tested and verified for the U.S. and Canadian governments, an important attribute for deploying mission-critical, highly secure mobile applications to the wide range of government organizations.

Validated FIPS 140-2 meets current and upcoming government security policy requirements as well as IEEE 802.11i and Wi-Fi Alliance WPA-2* compliance, which enables maximum security and interoperability with most WLAN infrastructures. They prevent cryptographic attacks as defined in FIPS 140-2 and can be used in non-FIPS environments, such as hot spots and home networks.



3 FIPS Validated Intel Wireless Adapters

FIPS 140-2 validated Intel wireless products enables federal government agencies to purchase and deploy laptop computers based on Commercial Off-The-Shelf (COTS) technology. Intel wireless clients are FIPS validated to deliver the compliance and requirements for achieving security, reliability, interoperability and assurance with the FIPS 140-1 and 140-2 standards.

3.1 Supported Operating Systems

Intel wireless adapters all support FIPS for the following operating systems:

- For Microsoft Windows XP* 32-bit– Use 3rd party FIPS client from 3eti or Cisco.
- For Microsoft Windows Vista* – FIPS natively supported in the operating system.
- For Microsoft Windows 7* – FIPS natively supported in the operating system.

3.2 FIPS Compliant Intel Wireless Products

The following table lists Intel wireless product FIPS solutions for Microsoft Windows XP, Microsoft Windows Vista and Microsoft Windows 7.

Intel Wireless Adapter	Microsoft Windows XP FIPS Solutions	Microsoft Windows Vista FIPS Solution	Microsoft Windows 7 FIPS Solution
Intel® WiFi Link 1000	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS support in operating system	Native FIPS support in operating system
Intel® WiFi Link 5100	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS support in operating system	Native FIPS support in operating system
Intel® WiFi Link 5300	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS support in operating system	Native FIPS support in operating system
Intel® WiMAX/WiFi Link 5350	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS (Wi-Fi) support in operating system	Native FIPS support in operating system
Intel® Centrino Wireless-N 1000	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS support in operating system	Native FIPS support in operating system
Intel® Centrino Advanced-N 6200	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS support in operating system	Native FIPS support in operating system
Intel® Centrino Ultimate-N 6300	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS support in operating system	Native FIPS support in operating system
Intel® Centrino Advanced-N + WiMAX 6250	Third-party FIPS solutions available for purchase from 3eti, Cisco	Native FIPS (Wi-Fi) support in operating system	Native FIPS support in operating system

3.3 Additional Intel Wireless Product Security

FIPS is an additional security requirement beyond wireless security technologies and standards. FIPS 140-2, IEEE 802.11i and WPA create the complete security package for Intel wireless LAN clients. Intel wireless adapters with Intel PROSet/Wireless software provide these security features:

- IEEE 802.11i (WPA/WPA2), IEEE 802.1X
- EAP-TLS
- WPA2 with up to 256-bit AES Security
- Public Key Infrastructure (PKI) with X.509 Certificates
- Common Criteria Compliance
- Layer 2 Security for Wireless Protection (separate from and independent of Layer 3 VPN design or architecture)
- DoD PKI [Joint Interoperability Test Command (JITC) certified] with password protection for multiple level authentication
- Availability of Custom DKE (Dynamic Key Exchange, per user, per session)
- Multiple location profiles
- Compatible with Virtual Private Networks (VPN)

4 Third-Party FIPS Client Software for Microsoft Windows XP

The Intel Wi-Fi driver is designed to work with FIPS certified libraries (version 13.1.1 or higher for Microsoft Windows XP). Third-party clients with FIPS certified libraries for Intel Wireless products in Microsoft Windows XP are available for purchase from 3eTi and Cisco.

For a complete FIPS validated solution, there must be a secure RADIUS server and FIPS validated Access Point for the clients to connect to.

4.1 3eTi

Intel wireless clients accompanied with 3e Technologies International* (3eTi) client software provides an optimal FIPS 140-2 validated client that is IEEE 802.11i-compliant and WPA2 certified. The Intel wireless client with the 3eTI client software seamlessly works with 3rd party vendor wireless access points for more secure wireless interoperability. The 3eTI client supports Microsoft Windows XP* and provides IEEE 802.11a/b/g wireless access along with enhanced protection through variety of cryptographic features that deliver a high level of security for wireless environments.

Intel wireless products are FIPS validated with the 3e Technologies International* (3eTI*) FIPS 140-2 Validated 3e-010F client software. This new capability enables U.S. Department of Defense (DoD) and other Federal users to employ secure wireless LAN systems using FIPS 140-2 Validated IEEE 802.11i technology.

Key 3eTI Product Features:

- Notebook-to-Network Security that encrypts voice, video and data communications between laptops and gateways / access points to protect confidentiality and prevent hacking
- Meets all current applicable government requirements documented on FIPS 140-2
- Additional security provided with 256-bit AES encryption and the Department of Defense PKI (Public Key Infrastructure) authentication

Note: For more information on the 3eTi FIPS client software, go to <http://www.efjohnsontechnologies.com/products/wirelessLAN/software>



4.2 Cisco

The Cisco Secure Services Client* is a software application that enables businesses of all sizes to deploy a single authentication framework across endpoint devices for access to both wired and wireless networks. The Cisco Secure Services Client solution delivers simplified management, robust security, and lower total cost of ownership. Through a simplified and scalable deployment mechanism, IT administrators can deploy and manage the Cisco Secure Services Client across the enterprise. The software client manages the user and device identity and the network access protocols required for secure access.

The Cisco Secure Services Client uses the IEEE 802.1X authentication standard to provide a robust first line of defense against unauthorized network intrusions. Using the 802.1X standard, access control decisions are made before the endpoint device is granted an IP address and access to the network. This gives the Cisco Secure Services Client the flexibility to deploy strong security for managing identity-based access for users and devices, and to deliver an effective port management solution. As a result, the operational cost of protecting the network is reduced.

Cisco Secure Services Client Version 5.1 contains an enterprise deployment feature that allows IT administrators to configure and deploy client profiles to the entire organization. Deploying the client from a centralized location saves significant time and ultimately helps lower the total cost of ownership (TCO) of deploying an 802.1X supplicant.

Federal Information Processing Standards (FIPS) drivers for Cisco's FIPS 140-2 Level 1 Compliant Solution is ordered separately.

Product Name	Part Number
Cisco Secure Services Client (Microsoft Windows XP)	AIR-SC5.0-XP2K
Cisco Secure Services Client (Microsoft Windows Vista)	AIR-SSC-VISTA
SSC FIPS Drivers (Microsoft Windows XP only)	AIR-SSCFIPS-DRV

Note: For more information on the Cisco Secure Services Client, visit http://www.cisco.com/en/US/prod/collateral/wireless/ps6442/ps7034/product_data_sheet0900aec805081a7.html

5 Conclusion

FIPS validated wireless LAN clients are frequently required by Federal, state and local government agencies. Intel wireless adapters support FIPS within the Microsoft Windows Vista and Microsoft Windows 7 Operating Systems. These solutions include the latest Intel® Centrino® Wireless LAN products: Intel® Centrino® Advanced-N 6200, Intel® Centrino® Ultimate-N 6300, and Intel® Centrino Advanced-N + WiMAX 6250. For Microsoft Windows XP, validated FIPS software can be purchased from 3eti and Cisco. For more information on Intel Wireless adapters, visit <http://www.intel.com/network/connectivity/products/wireless/index.htm?iid=go+wifi>