Laird TECHNOLOGIES

Innovative **Technology** for a **Connected** World

FIPS 140-2 and Wi-Fi Client Devices

Originally Published: April 2012

Updated: October 2012

A White Paper from Laird Technologies

With throughput much greater than that available with previous wireless local area networking (WLAN) standards, the IEEE 802.11n standard has had a significant impact on the WLAN, or Wi-Fi, industry. Most of today's WLAN infrastructure products support 802.11n, and support on client devices is growing.

Putting 802.11n on laptops and other general-purpose client devices makes sense if those devices need a throughput boost. Most medical devices don't need higher throughput. Because those devices may be used for five years or longer, consider dual-band 802.11n for them now if you can get it for a modest price premium.

Americas: +1-800-492-2320 Option 3
Europe: +44-1628-858-940
Hong Kong: +852-2268-6567 x026
www.lairdtech.com/wireless

Contents

EXECUTIVE SUMMARY

AES-CCMP is an approved cryptographic method for FIPS 140-2, which defines the standard for cryptographic modules that protect sensitive but unclassified information. Since 2006, support for AES-CCMP has been a requirement for Wi-Fi® certification, so nearly every Wi-Fi chip supports AES-CCMP in hardware, i.e. on the chip. Very few Wi-Fi products, however, are validated for FIPS 140-2, primarily because Wi-Fi chips lack support for loopback, which is required for some FIPS 140-2 validation tests. Alternatives to chip-based AES-CCMP for FIPS 140-2 involve software cryptography, which is ill-suited to devices that have relatively modest CPU and memory resources or require long battery life. Organizations considering FIPS 140-2 for Wi-Fi client devices should consider whether or not WPA2™-Enterprise with chip-based AES-CCMP provides sufficient security.

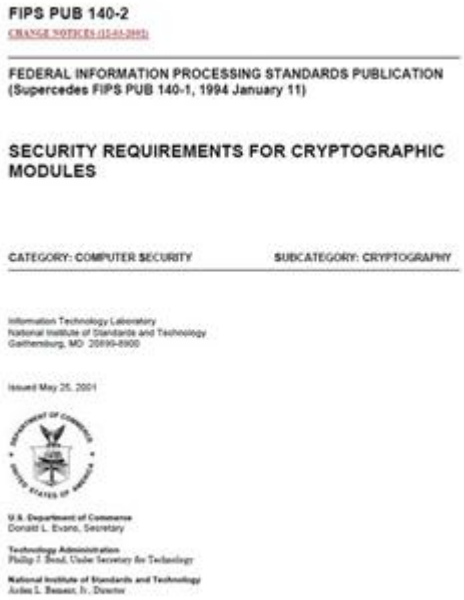
FIPS 140-2

Overview

Federal Information Processing Standards (FIPS) publications are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce. Issued May 25, 2001, FIPS 140-2 is a FIPS publication that defines the standard for cryptographic modules used within a security system that protects sensitive but unclassified information. The FIPS 140-2 publication is the second version of the publication; it supersedes the first version, FIPS 140-1, in its entirety. The remainder of this document uses the term FIPS 140-2 to refer to the standard, not the publication.

FIPS 140-2 security requirements cover the following areas related to the secure design and implementation of a cryptographic module:

- Cryptographic module specification
- Cryptographic module ports and interfaces
- Roles, services, and authentication
- A finite state model for the cryptographic module
- Physical security for the module
- The module's operational environment
- How cryptographic keys are managed
- Electromagnetic interference and electromagnetic compatibility (EMI/EMC)
- Self-tests
- Design assurance
- Mitigation of other attacks


FIPS PUB 140-2

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. A joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada, CVMP strives to promote the use of validated cryptographic modules in equipment procured by Federal agencies. FIPS 140-2 validation testing of cryptographic modules is performed by independent testing laboratories that are accredited by the National Voluntary Laboratory Accreditation Program (NVLAP).

Self-Tests

FIPS 140-2 compliance requires the execution of self-tests, which are designed to ensure that the cryptographic module is functioning properly. Two types of self-tests are required:

1. Power-up self-tests, which are performed when the module is powered up
2. Conditional self-tests, which are performed when an applicable security function or operation is invoked.

A power-up test must be initiated automatically, not requiring operator intervention. While the test runs, there can be no data output via the data output interface. When the test completes, the indication of success or failure must be output via the "status output" interface. There are three types of power-up tests for a cryptographic module:

1. Cryptographic algorithm test: For each cryptographic algorithm in a module, this test, also called a known-answer test (KAT), is conducted for all cryptographic functions such as encryption, decryption, authentication, and random number generation. Data for which the correct output is known is input into the algorithm, and the calculated output is compared to the known answer. If the output of an algorithm varies for a given set of inputs, then the algorithm may be tested using a pair-wise consistency test.
2. Software/firmware integrity test: This test is run against all software and firmware components of a module. In some cases, a digital signature test may suffice.
3. Critical functions test: This test applies to any other security functions that are critical to the secure operation of a cryptographic module.

The following conditional self-tests may be required for a cryptographic module:

- Pair-wise consistency test: Required if the module generates public or private keys.
- Software/firmware load test: Required if software or firmware components can be externally loaded into the module.
- Manual key entry test: Required if cryptographic keys or key components are manually entered into the module.
- Continuous random number generator (RNG) test: Required if the module employs RNGs in an approved mode of operation.
- Bypass test: Required if the module implements a bypass capability whereby the services may be provided without cryptographic processing (e.g., transferring plaintext through the module).

Wi-Fi Cryptography: AES-CCMP

Wi-Fi is the common name for wireless local area networking that adheres to IEEE 802.11 standards. An industry consortium known as the Wi-Fi Alliance® promotes the use of Wi-Fi by offering the Wi-Fi CERTIFIED™ seal to products that pass a set of interoperability tests. An additional requirement for every product seeking the Wi-Fi CERTIFIED seal is to pass a security certification program called WPA2, which is based on the ratified IEEE 802.11i standard.

The IEEE began developing the 802.11i standard in the early 2000s, when it was determined that the original Wi-Fi security mechanism of Wired Equivalent Privacy (WEP) was insufficient for several reasons, including:

- **No access control:** While it defines a means to scramble, or encrypt, transmitted data, WEP provides no means to control access to a WLAN. If you know the WEP encryption key, then you can gain access to the WLAN.
- **Vulnerable keys:** Due to weaknesses in WEP, a hacker can "crack" or decipher a WEP key by collecting WEP-encrypted data packets and running them through a WEP-cracking tool. Today, using sophisticated tools, even a 104-bit WEP key can be cracked in less than an hour.
- **Static keys:** The only way to avoid the use of a WEP key that has been cracked by a hacker is to change all WEP keys regularly, which today means more frequently than every hour. Because the most common way of deploying WEP keys is to define them statically on all devices that used them, changing WEP keys is an administrative nightmare.

While the IEEE 802.11i task group worked to finalize a new Wi-Fi security standard, the Wi-Fi Alliance introduced an interim security certification called Wi-Fi Protected Access, or WPA™. There are two versions of WPA: Personal and Enterprise. Each defines a process for mutual authentication between the Wi-Fi client and the Wi-Fi infrastructure. At the end of the authentication process, a key is derived dynamically from the information exchanged between the client and the infrastructure. After the authentication process completes, the derived key is used to encrypt and decrypt all unicast data that travels between the client and the infrastructure.

Because WPA was designed to be supported by existing Wi-Fi products that support WEP, the encryption method in WPA, called TKIP, uses the same RC4 algorithm as WEP. Several researchers have published papers touting a vulnerability in TKIP.

Shortly after the IEEE approved the full 802.11i specification in July 2004, the Wi-Fi Alliance introduced a new interoperability testing certification, called WPA2, which incorporates the key elements of 802.11i. WPA2 is essentially the same as WPA, with TKIP replaced by a stronger encryption method based on the Advanced Encryption Standard (AES) cipher. In March 2006, WPA2 certification became mandatory for all new equipment certified by the Wi-Fi Alliance.

As with WPA, there are two versions of WPA2, Personal and Enterprise. The Enterprise versions of WPA and WPA2 are shown in Figure 1. The primary difference between the two is the method of encryption: TKIP for WPA-Enterprise and AES-CCMP for WPA2-Enterprise.[1]

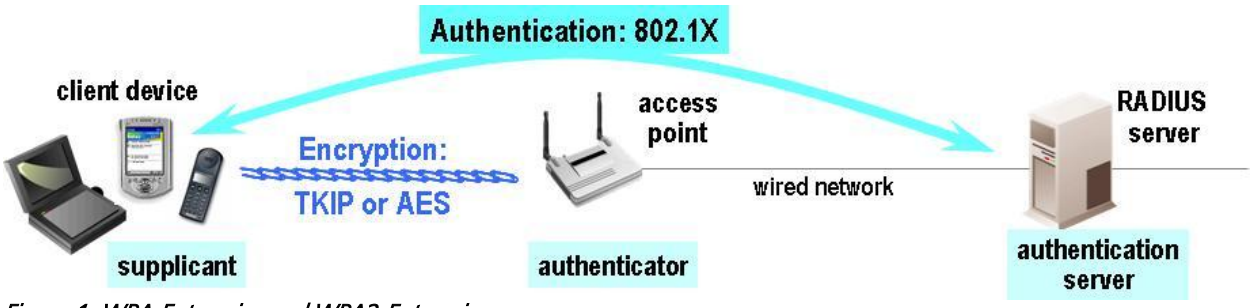


Figure 1: WPA-Enterprise and WPA2-Enterprise

[1] AES-CCMP can be used with WPA and TKIP can be used with WPA2, but the use of AES-CCMP with WPA2 is consistent with the definition of 802.11i.

AES-CCMP does not have the vulnerabilities of TKIP. The Wi-Fi Alliance promotes AES-CCMP as a "government-grade" encryption method that was developed by NIST and is "compliant" with FIPS 140-2. According to FIPS 140-2 Annex A, AES-CCMP is an approved security function for use in a FIPS-approved mode of operation.

WPA2 and FIPS 140-2

Most organizations that require FIPS 140-2 for Wi-Fi client devices have configured their Wi-Fi networks for WPA2-Enterprise and want client devices to use WPA2-Enterprise. To be validated for FIPS 140-2, the WPA2-Enterprise implementation on a client device must meet these requirements:

- Support WPA2-Enteprise authentication and key derivation using a FIPS-validated software module in a FIPS-approved mode of operation.
- Encrypt and decrypt all transmitted data using AES-CCMP through a FIPS-validated hardware or software cryptographic module.

Supplicant: Authentication and Key Derivation

The role of the supplicant, a security application that runs on a Wi-Fi client device, is to perform 802.11i authentication and encryption key derivation. According to a NIST document[2] that provides FIPS 140-2 implementation guidance (IG), the IEEE 802.11i standard describes how to derive keys from a secret shared between two parties but does not specify how to establish this commonly shared secret. A cryptographic module can use the 802.11i key derivation techniques to derive a data protection key, a key encryption key, and other keys for use in a FIPS-approved mode of operation, provided that the following are true:

- The shared secret (the keying material) must be established using a FIPS-approved method specified in FIPS 140-2 Annex D.
- The key derivation function must be implemented as defined in the NIST IG document.
- If the keying material is established via a manual method, then the method must be specified in FIPS 140-2, and a key derivation function as defined in the NIST IG document can be applied.

In the 802.11i authentication process, the Extensible Authentication Protocol (EAP) method is used to establish a shared secret, and an 802.11i handshake establishes the key that is used for AES-CCM encryption. Initially, only EAP-TLS was allowed using RSA for establishing a shared secret. Today, more EAP methods are allowed, but all are based on TLS.

A FIPS-validated module must be used for the 802.11i handshake, the 802.11i EAPOL-KEY message integrity check (MIC) generation, encryption/decryption, and random generation. This module must support the following crypto operations:

- Key material generation using a pseudo-random function that uses HMAC-SHA1
- Nonces generated using pseudo-random data
- EAPOL-key MIC generated using HMAC-SHA1-128
- EAPOL-key encrypted data using NIST AES key wrap

[2] http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

AES-CCMP in Hardware

Because WPA2 is a requirement for Wi-Fi certification, the vast majority of today's Wi-Fi chips support the WPA2 cryptographic algorithm, AES-CCMP, in hardware (on the Wi-Fi chip itself). Chip-based cryptography provides a significant performance benefit because the CPU, memory, and battery resources of the client device are not used when encrypting and decrypting data packets.

As mentioned in the section on self-tests, if a chip-based AES-CCMP module is to be validated for FIPS 140-2, then the device that uses the chip must be able to conduct self-tests on the module, both at power-up and when applicable security functions or operations are invoked. Power-up self-tests include a KAT that must be conducted for all cryptographic functions, such as encryption and decryption. With a KAT, data for which the correct output is known is input into the module, and the calculated output is compared to the known answer.

In normal Wi-Fi operation, the chip-based AES-CCMP module on a client device is used to encrypt data only when the client is sending data to an access point (AP), and the module is used to decrypt data only when the client receives data from an AP. With a self-test for encryption, data is not sent to an AP but must be examined on the client device. With a self-test for decryption, data is not received from an AP but is supplied by the client device.

To enable self-tests to be performed, the Wi-Fi chip must support a loopback mechanism. After encrypting data for a self-test, the chip loops the encrypted data to the self-test (on the client device) rather than transmitting the data to an AP. When a self-test for decryption is being conducted, the chip must recognize that the encrypted data is coming not from an AP but from the self-test (on the client device); after decrypting the data, the chip must supply that data to the self-test.

Very few Wi-Fi chips used in client devices support a loopback mechanism. As a result, very few – and possibly no – Wi-Fi client devices have been validated for FIPS 140-2 using a chip-based AES-CCMP module.

AES-CCMP in Software

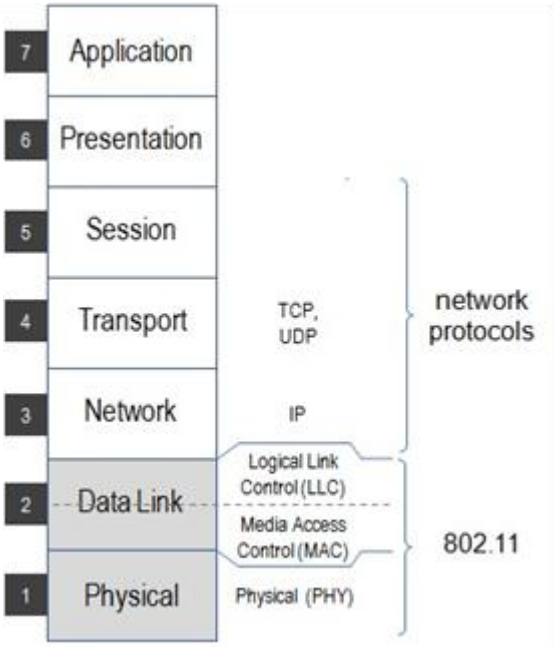
When chip-based AES-CCMP cannot be validated for FIPS 140-2, an AES-CCMP software module is a possible alternative. Software modules that perform AES-CCMP encryption and decryption made their debut after IEEE 802.11i was ratified in 2004. Once WPA2 became a Wi-Fi certification requirement in 2006, the majority of chips began to support AES-CCMP in hardware. Devices with older chips, however, usually lacked hardware support for AES-CCMP. Rather than replacing older devices, some organizations opted to run software cryptographic modules with AES-CCMP support. Some of those modules achieved FIPS 140-2 validation.

The 802.11 security configuration on the client device needs to match that on the AP with which the client is communicating. When WPA2 is configured on both, the 802.11 header in every transmitted packet indicates that the packet is encrypted. A client device can use a software AES-CCMP module with a chip that supports AES-CCMP in hardware only if that chip provides a mechanism to turn off the chip-based AES-CCMP and use software-based AES-CCMP instead. The software module must be used to encrypt every data packet that the chip transmits to the AP and decrypt every data packet that the chip receives from the AP.

One commercial product that includes an AES-CCMP software module that is validated for FIPS 140-2 is Juniper Network Odyssey Access Client FIPS Edition. Windows 7 and Windows Embedded Handheld include a FIPS-validated AES-CCMP cryptographic module called the Microsoft Crypto Next Generation (CNG) software[3] module. Under the **802.11 settings** tab in the **Advanced settings** window of Windows 7, there is a checkbox for "Enable Federal Information Processing Standard (FIPS) compliance for this network". If that checkbox is checked, then Windows 7 uses its AES-CCMP module to "perform AES encryption in a FIPS 140-2 certified mode." Other FIPS-validated AES-CCMP software modules include RSA BSAFE and Mocana NanoCrypto.

The use of software cryptography instead of chip-based cryptography on a client device with relatively modest CPU and memory resources may result in performance problems, as the CPU and memory may be taxed in encrypting or decrypting every data packet. When the client device has stringent battery life requirements, those requirements may not be met when software cryptography is used, as the encryption and decryption may consume too much battery power.

AN ALTERNATIVE TO WPA2-ENTERPRISE: VPN



Error! Reference source not found. shows the seven-layer OSI model. WPA2-Enterprise operates at Layer 2, the Data Link layer. Other security schemes operate at higher layers. When WPA2-Enterprise cannot be validated for FIPS 140-2, NIST suggests[4] the use of a virtual private network (VPN) for all Wi-Fi communications, provided that the VPN uses a FIPS-validated encryption algorithm contained in a validated cryptographic module.

A VPN is a virtual network, built on top of an existing and typically untrusted physical network, that provides a secure communications mechanism at Layer 3. To use a VPN to protect IP traffic that is sent over a Wi-Fi link, you must establish a VPN tunnel between the Wi-Fi client device and a VPN concentrator that is on the network behind the AP with which the client is communicating. VPN security services are provided not at Layer 2 but at Layer 3, so the VPN secures all applications and protocols operating at Layer 3 and above. Two popular VPN technologies are Internet Protocol Security (IPSec) VPNs and Secure Sockets Layer (SSL) VPNs.

Figure 2: Wi-Fi in the OSI model

The list[5] of cryptographic modules that have been validated for FIPS 140-2 includes many virtual private network (VPN) clients. In fact, the list uses a VPN client as an example of cryptographic module that often is validated for FIPS 140-2.

[3] The CNG software library may be able to leverage a hardware implementation of AES-CCMP.

[4] http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

[5] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

With a VPN, cryptography on the client device is performed not in hardware but in software. As was mentioned earlier, the use of software cryptography on a client device with relatively modest CPU and memory resources may result in performance problems and may tax the battery of a battery-powered device. When you rely on a VPN for every connection to the enterprise Wi-Fi network, your IT staff must:

- Configure a VPN client on every Wi-Fi client device and ensure that the device uses the VPN client when connecting to the enterprise Wi-Fi network.
- Ensure that a VPN concentrator is configured "behind" every AP on your enterprise Wi-Fi network so that, if a Wi-Fi client device connects to an AP, then that device can gain access to the enterprise network only by going through the VPN concentrator.

IS WPA2-ENTERPRISE SUFFICIENT?

Today, most organizations that use Wi-Fi rely on WPA2-Enterprise for robust, standards-based security on their Wi-Fi networks. Those organizations that want FIPS 140-2 validation for their Wi-Fi client devices would prefer that FIPS-validated cryptography leverages the WPA2-Enterprise configuration that is in place already. In other words, these organizations want to use FIPS-validated AES-CCMP to encrypt and decrypt all Wi-Fi data at Layer 2.

Nearly every Wi-Fi chip provides hardware support for AES-CCMP, but few of the chips designed for client devices support loopback, which is required for FIPS 140-2 self-tests. Laird Technologies has been unable to find a single FIPS-validated Wi-Fi client device for which chip-based AES-CCMP has been FIPS-validated. The only FIPS-validated cryptographic modules for Wi-Fi client devices are software modules, such as AES-CCMP software modules (which require that chip-based AES-CCMP is disabled) and VPN clients.

Software cryptography is ill-suited to devices that have relatively modest CPU and memory resources or require long battery life. Organizations considering FIPS 140-2 for Wi-Fi client devices should consider whether or not WPA2-Enterprise with chip-based AES-CCMP is sufficient to protect sensitive but unclassified information