# Airespace Cryptographic Manager (ACM)

# Security Policy

Document Version 1.3

March 5. 2004

## Airespace, Inc.

 

# Security Policy

## 1 Purpose and Scope

This document has been created as part of the process of submitting the Airespace Cryptographic Manager (ACM) (HW P/N AS-4101, AS-4012, AS-4024 Version 1.0; FW Version 1.2.77.4) to the FIPS-140-2 [FIPS-140-2] validation process. It documents the *Security Policy* for the ACM.

- The security policy consists of a specification of the security rules under which a cryptographic module shall operate.

## 2 Table of Contents



 

# 3 Product overview

The *Airespace Cryptographic Manager* (ACM) is a collection of hardware and firmware components that is sold in different models of a product that is generally called an *Airespace Switch*. The specific models covered by the FIPS-140-2 validation are described in Section 4.5.

**Figure 1. Airespace Switch 12-port and 24-port models**

**Figure 2. Airespace Appliance with Fiber Optic Port**

The Access Point transceivers mentioned in this document are not part of the ACM.

 

# 4 Module Objectives

This section describes the assurance levels being pursued for each of the major requirement areas in the FIPS-140-2 standard. It also describes the set of FIPS standard security mechanisms that are used by the module.

## *4.1 Security Levels*

The following table specifies the security level the vendor is pursuing for each major requirement area of the FIPS 140-2 standard. The overall security level for the ACM is Level 2.

**Table 1. Assurance Objectives for Major Requirement Areas**

| | |
|---|---|
| 1. Cryptographic Module Specification: | Level 2 |
| 2. Module Ports and Interfaces: | Level 2 |
| 3. Roles, Services, and Authentication: | Level 2 |
| 4. Finite State Model: | Level 2 |
| 5. Physical Security: | Level 2 |
| 6. Operational Environment: | N/A |
| 7. Cryptographic Key Management: | Level 2 |
| 8. EMI/EMC | Level 2 |
| 9. Self-Tests: | Level 2 |
| 10. Design Assurance: | Level 2 |
| 11. Mitigation of Other Attacks: | N/A |

 

## 4.2 Modes of Operation

The module supports both a FIPS approved mode of operation and a non-approved mode. This section briefly explains how to put the module into the FIPS approved mode, and how to determine if the module in is operating in the FIPS mode.

After following the basic installation instructions in the module's User Manual, the External Crypto Officer (ECO) performs the following steps.

1. Establish a TLS connection to the module via the Management Network Port.
2. User the factory default password for the Admin account to login.
3. Change the Admin account password to a hard to guess value that is more than 8 characters long.
4. Set the Network Layer 2 security to "None" (don't use 802.11 encryption).
5. Set the Network Layer 3 security to "IPSec" (require IPSec encryption for all User role data).
6. Set the User Authentication to "XAuth Pre-Shared Key" and disable Radius authentication.
7. Terminate the TLS session.

The ECO can determine that the module is operating in the FIPS approved mode by performing the following steps.

1. Establish a TLS connection to the module via the Management Network Port.
2. Login with the ECO password.
3. Check that the Network Layer 2 security is "None" (don't use 802.11 encryption).
4. Check that the Network Layer 3 security is "IPSec" (require IPSec encryption for all User role data).
5. Check that the User Authentication is "XAuth Pre-Shared Key" and that Radius authentication is disabled.
6. Terminate the TLS session.

 

## 4.3 FIPS Approved Security Mechanisms

The module uses the following FIPS approved security mechanisms.

1. TDES-CBC with three keys as specified in [FIPS-46-3].
2. AES-CBC with 128-bit keys as specified in [FIPS-197].
3. SHA-1 on byte boundary data as specified in [FIPS-180-2].
4. HMAC-SHA-1 with 160-bit keys as specified in [FIPS-198].
5. RSA With SHA-1 signature generation and verification with 1024-bit and 1536-bit RSA keys as specified in [FIPS-186-2].
6. Commercial key establishment protocols (TLS, IPSEC/IKE and LWAPP) using appropriate cipher suites for FIPS-140-2.
7. Deterministic Random Number Generation (DRNG) using FIPS approved algorithms. One DRNG uses the ANSI X9.31 Appendix A algorithm, the other uses the FIPS-186-2 Appendix 3.1 algorithm based on SHA-1.
8. RSA key-pair generation using approved DRNG and conditional test for pair-wise consistency. The RSA keys for TLS are generated with the FIPS 186-2 DRNG, and the RSA keys for IPSec are generated with the X9.31 DRNG.
9. Generation of initialization vectors (IVs) and random nonce values using FIPS approved DRNG. The IVs and nonces for TLS and LWAPP are generated by the FIPS-186-2 DRNG. The IVs and nonces for IPSec are generated by the X9.31 DRNG. The generation of session keys for LWAPP (for AES and HMAC-SHA-1) are performed with the FIPS 186-2 DRNG.

The module supports the following FIPS Approved algorithms:

- Triple-DES
- AES
- SHA-1
- HMAC-SHA-1 (vendor affirmed)
- RSA Sign/Verify (PKCS #1, vendor affirmed)
- RSA Key Wrapping (PKCS #1, vendor affirmed)
- FIPS 186-2 DRNG Appendix 3.1 with underlying G-function constructed from SHA-1
- ANSI X9.31 DRNG

The module supports the following non-Approved algorithms:

- RC4
- MD5
- Diffie-Hellman (commercially available key establishment)

 

## 4.4 Strength of FIPS Approved Cryptographic Mechanisms

The cryptographic module provides 80-bits of security. The module should only be used in environments where an effective key strength of 80-bits meets the security requirements of the end users of the system.

 

## 4.5 Hardware Platforms

The ACM is branded and sold as Airespace Switch for marketing purposes. The models that are covered by this validation include both the 12-port and 24-port models with three options for the Gigabit Network Interface Card (none, copper wire interface, and fiber-optic interface). The module has an internal option for two different power supplies (low wattage and high wattage) depending on whether the RJ45 ports will provide power to an external device (Power Over Ethernet). Both power supply options will be evaluated.

The firmware for all platforms is the same. The version number for this firmware is "1.2.77.4".

In total thirteen hardware platforms are included in the validation.

The following table provides the identification for all the modules being validated.

**Table 2. Identification of Hardware Configurations**

| **Hardware Version Numbers** | **Hardware Configuration Options**<br>All configurations include a DB-9 console port, an RJ45 management port, three status LEDs and a power cord receptacle. |
|---|---|
| AS-4012-00S00 | 12 RJ-45 wireless ports, no Gigabit card, low wattage power supply. |
| AS-4012-0PS00 | 12 RJ-45 wireless ports, no Gigabit card, high wattage power supply. |
| AS-4012-X0S00 | 12 RJ-45 wireless ports, Fiber-Optic Gigabit card, low wattage power supply. |
| AS-4012-XPS00 | 12 RJ-45 wireless ports, Fiber-Optic Gigabit card, high wattage power supply. |
| AS-4012-T0S00 | 12 RJ-45 wireless ports, Copper-Wire Gigabit card, low wattage power supply. |
| AS-4012-TPS00 | 12 RJ-45 wireless ports, Copper-Wire Gigabit card, high wattage power supply. |
| AS-4024-00S00 | 24 RJ-45 wireless ports, no Gigabit card, low wattage power supply. |
| AS-4024-0PS00 | 24 RJ-45 wireless ports, no Gigabit card, high wattage power supply. |
| AS-4024-X0S00 | 24 RJ-45 wireless ports, Fiber-Optic Gigabit card, low wattage power supply. |
| AS-4024-XPS00 | 24 RJ-45 wireless ports, Fiber-Optic Gigabit card, high wattage power supply. |
| AS-4024-T0S00 | 24 RJ-45 wireless ports, Copper-Wire Gigabit card, low wattage power supply. |
| AS-4024-TPS00 | 24 RJ-45 wireless ports, Copper-Wire Gigabit card, high wattage power supply. |
| AS-4101-X0S00 | No RJ-45 wireless ports, Fiber-Optic Gigabit card, low wattage power supply. |

 

# 5 Roles and Authentication

The module supports the following three roles.

1. User Role. This role performs general security services including cryptographic operations and other approved security functions.
2. Inter-module Crypto Officer (ICO) Role. This role performs the "mobility" service, which securely transfers session keys from one module to another.
3. External Crypto Officer (ECO) Role. This role performs the cryptographic initialization and management operations. In particular, it performs the loading of optional certificates and key-pairs and the zeroization of the module.

The module does not support a maintenance role.

## *5.1 Identification and Authentication Policy*

The module supports role-based authentication as allowed for FIPS-140-2 Level 2 assurance.

The module supports concurrent operators that are kept separate using the process and threading mechanisms provided by the firmware. All previous authentication status information is cleared on power-on. Re-authentication is required to change roles.

The following table explains the roles and their related identification and authentication information. The table after this one explains the effective strength of each authentication.

**Table 3. Roles and Required Identification and Authentication**

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| User | Role-Based Operator Identification | 1) IPSec User role pre-shared key, or<br>2) IPSec User role certificate |
| Inter-module Crypto Officer | Role-Based Operator Identification | 1) IPSec ICO role certificate, or<br>2) LWAPP ICO role certificate. |
| External Crypto Officer | Role-Based Operator Identification | ECO Password |

 

**Table 4. Strengths of Authentication Mechanisms**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| IPSec User role pre-shared key | Random guess being correct is 1 in $90^{13}$, which is roughly 1 in $2.5 \times 10^{25}$. This is much stronger than the 1 in $1 \times 10^{6}$ required by FIPS-140-2. The chance of this succeeding in any one minute is 1000 in $90^{16}$, which is roughly 1 in $2.5 \times 10^{22}$. This is much stronger than the 1 in $1 \times 10^{5}$ required by FIPS-140-2. |
| IPSec User role certificate | The chance of a random guess being correct is 1 in $2^{80}$, which is roughly 1 in $1.2 \times 10^{24}$. This is much stronger than the 1 in $1 \times 10^{6}$ required by FIPS-140-2. The chance of this succeeding in any one minute is 1000 in $2^{80}$, which is roughly 1 in $1.8 \times 10^{21}$. This is much stronger than the 1 in $1 \times 10^{5}$ required by FIPS-140-2. |
| IPSec ICO role certificate | The chance of a random guess being correct is 1 in $2^{80}$, which is roughly 1 in $1.2 \times 10^{24}$. This is much stronger than the 1 in $1 \times 10^{6}$ required by FIPS-140-2. The chance of this succeeding in any one minute is 1000 in $2^{80}$, which is roughly 1 in $1.8 \times 10^{21}$. This is much stronger than the 1 in $1 \times 10^{5}$ required by FIPS-140-2. |
| LWAPP ICO role certificate | The chance of a random guess being correct is 1 in $2^{80}$, which is roughly 1 in $1.2 \times 10^{24}$. This is much stronger than the 1 in $1 \times 10^{6}$ required by FIPS-140-2. The chance of this succeeding in any one minute is 1000 in $2^{80}$, which is roughly 1 in $1.8 \times 10^{21}$. This is much stronger than the 1 in $1 \times 10^{5}$ required by FIPS-140-2. |
| ECO Password | The chance of a random guess being correct is 1 in $90^{8}$, which is roughly 1 in $4.3 \times 10^{15}$. This is much stronger than the 1 in $1 \times 10^{6}$ required by FIPS-140-2. The chance of this succeeding in any one minute is 1000 in $90^{8}$, which is roughly 1 in $4.3 \times 10^{12}$. This is much stronger than the 1 in $1 \times 10^{5}$ required by FIPS-140-2. |

 

# 6 Description of Security Services

The following table provides brief descriptions of all the security services supported by the module.

**Table 5. Description of Security Services**

| Service Name | Service Description |
|---|---|
| Module Self-Test & Initialize | Performs self-tests, zeroizes all CSPs store in RAM, clears information about authenticated external operators, and if successful, the module enters its Ready state. This is also the service used to recover from the FIPS Error state. |
| Module Show Status | Displays indication of module state (Uninitialized, Ready or Error) and the module mode (this version can only be in FIPS mode). The state is also indicated through an LED on the module front panel. The LED is red when Uninitialized (during power-up self-test), black when Ready, and red when in the Error state. |
| Radio Resource Management | Display and automatically configure radio parameters including transmitter power, receiver sensitivity, and RF frequency. This service does not use any cryptographic algorithms. |
| Zeroize CSP | Zeroizes all CSPs stored in RAM and flash ROM including resetting the password for the External Crypto Officer role to its default value. This service is performed in two steps by the ECO role executing a command and then power-cycling the module. |
| Change ECO Password | Changes the External Crypto Officer role password. |
| Generate RSA Key Pair | Generate an RSA public and private key pair and self-signed certificate for use with TLS. |
| Load RSA Key & Cert | Load an RSA public key in a certificate with optional private key. This can set the public key for verifying User role IPSec certificates. It can set the key-pair and certificate for authenticating the module for IPSec User role connections or for TLS ECO role connections. |
| Update Firmware | Update firmware image if it is properly signed by Airespace. The ECO must ensure that the new image has received a FIPS-140-2 validation. |
| Set IPSec/IKE Pre-Share Key | Sets the IPSec/IKE pre-shared key for this commercially available key agreement protocol using an appropriate FIPS cipher suite and authenticate for the User role. |
| IPSec/IKE Session Establishment for ICO role | Implement the commercially available key agreement protocol for IPSec/IKE using an appropriate FIPS cipher suite and authentication for the ICO role. |
| IPSec Session Data Transfer for ICO role | Transfer data and CSP via IPSec in the ICO role. |

 

| Service Name | Service Description |
|---|---|
| Transfer IPSec session for User role | The ICO role operator uses this service to transfer the IPSec User role session keys and configuration between ACM modules to support the mobility of User sessions between ACM modules. |
| IPSec/IKE Session Establishment for User role | Implement the commercially available key agreement protocol for IPSec/IKE using an appropriate FIPS cipher suite and authenticate for the User role. |
| IPSec Session Data Transfer for User role | Transfer data via IPSec in the User role. |
| TLS Session Establishment for ECO role | Implement the commercially available key agreement protocol for TLS using an appropriate FIPS cipher suite and authenticate for the ECO role. |
| TLS Session Data Transfer for ECO role | Transfer data and CSP via TLS. |
| LWAPP Session Establishment for ICO role | Implement the commercially available key agreement protocol for LWAPP using an appropriate FIPS cipher suite and authenticate for the ICO role. |
| LWAPP Session Data Transfer for ICO role | Transfer control and status information to and from Access Point devices via LWAPP in the ICO role. |

The module does not support a bypass capability. The implementation of all services begin by checking whether the module is in the FIPS Error state, and return an error if it is. This prevents the module from performing input or output in the FIPS Error state.

 

# 7 Security Services by Role Policy

This section describes the policy that governs which services can be performed by each role. The following table lists all the security services and indicates whether an operator each role can perform that service.

**Table 6. Security Services Allowed by Role**

| Service Name | User | Inter-module Crypto Officer | External Crypto Officer |
|---|---|---|---|
| Module Self-Test & Initialize | Yes | Yes | Yes |
| Module Show Status | Yes | Yes | Yes |
| Radio Resource Management | Yes | Yes | Yes |
| Zeroize CSP | No | No | Yes |
| Change ECO Password | No | No | Yes |
| Generate RSA Key Pair | No | No | Yes |
| Load RSA Key & Cert | No | No | Yes |
| Update Firmware | No | No | Yes |
| Set IPSec/IKE Pre-Share Key | No | No | Yes |
| IPSec/IKE Session Establishment for ICO role | No | Yes | No |
| IPSec Session Data Transfer for ICO role | No | Yes | No |
| Transfer IPSec session for User role | No | Yes | No |
| IPSec/IKE Session Establishment for User role | Yes | No | No |
| IPSec Session Data Transfer for User role | Yes | No | No |
| TLS Session Establishment for ECO role | No | No | Yes |
| TLS Session Data Transfer for ECO role | No | No | Yes |
| LWAPP Session Establishment for ICO role | No | Yes | No |
| LWAPP Session Data Transfer for ICO role | No | Yes | No |

Three of the services do not require authentication to perform. The Module Self-Test and Initialize service can be performed by power-cycling the module, but it does require physical access to the module. It can also be performed by the warm reset command by an authenticated ECO. The Module Show Status service can be performed by observing the FIPS Error LED on the front panel. The Radio Resource Management service is performed without any authentication based on information received by the Access Point devices that are outside of the module boundary.

 

# 8 Critical Security Parameters (CSP)

This section lists the Critical Security Parameters for the module. The following table names and briefly describes each one.

**Table 7. Description of Critical Security Parameters**

| Key | Description/Usage |
|---|---|
| ECO Password | Authentication data for ECO role. |
| IPSec Private Key for ICO role | 1536-bit RSA private key used for IPSec Commercially Available Key Establishment protocol to authenticate ICO role. |
| IPSec Pre-Shared Key for User role | Key for IPSec Commercially Available Key Establishment protocol to authenticate User role. |
| IPSec Private Key for User role | Optional 1024-bit RSA private key used for IPSec Commercially Available Key Establishment protocol to authenticate User role when pre-shared key is not used. |
| TLS Private Key | 1024-bit RSA private key used for TLS Commercially Available Key Establishment protocol |
| IPSec Encryption Key | 128-bit AES key or 168-bit TDES key used to encrypt session data. |
| IPSec Integrity Key | 160-bit HMAC-SHA-1 key for tamper protection of session data. |
| TLS Pre-Master Secret | Shared secret created using asymmetric cryptography from which new TLS session keys can be created. |
| TLS Encryption Key | 128-bit AES key or 168-bit TDES key used to encrypt session data. |
| TLS Integrity Key | 160-bit HMAC-SHA-1 key for tamper protection of session data. |
| Access Point Encryption Key | 128-bit AES key used to encrypt Access Point control information. |
| Access Point Integrity Key | 160-bit HMAC-SHA-1 key for tamper protection of Access Point control information. |
| DRNG Key for X9.31 Appendix A algorithm | 168-bit seed key and 64-bit state for X9.31 DRNG algorithm. |
| DRNG Key for FIPS-186-2 Appendix 3.1 algorithm | 256-bit seed key for FIPS-186 DRNG algorithm. |
| Diffie-Hellman Private Key | Used for commercially available key establishment protocol. |
| IKE Encryption Key | 128-bit AES key or 168-bit TDES key used to encrypt session data. |
| IKE Integrity Key | 160-bit HMAC-SHA-1 key for tamper protection of session data. |

 

The following table describes the public keys that are used by the module. These are not CSP values, but they are important to understanding the overall security of the module.

**Table 8. Description of Public Keys**

| Key | Description/Usage |
|---|---|
| Airespace Root Certificate Verification Public Key | 1536-bit RSA public key used to verify signatures on certificates issued by Airespace. |
| Firmware Signature Verification Public Key | 1536-bit RSA public key used to verify signatures on updates to the module's firmware. |
| Device Certificate Verification Public Key | 1536-bit RSA public key used to verify signatures on IPSec certificates from other ACM modules and from the Access Point devices. |
| IPSec Public Key for ICO role | 1536-bit RSA public key for this ACM module used with the IPSec commercially available key establishment protocol to authenticate ICO role session to other ACM modules. |
| IPSec User Certificate Verification Public Key | Optional 1024-bit RSA public key used to verify signatures on IPSec User role certificates received by the module when the pre-shared key is not used for authenticating the User role. |
| IPSec Public Key for User role | Optional 1024-bit RSA public key for this ACM module used for IPSec commercially available key establishment protocol to authenticate User role sessions when the pre-shared key is not used for authenticating the User role. |
| TLS Public Key | 1024-bit RSA public key for this module used for TLS commercially available key establishment protocol. |
| Diffie-Hellman Public Key | Used for commercially available key establishment protocol. |

 

# 9 CSP by Service Policy

The following table presents the policy controlling which Critical Security Parameters are accessed by each service.

**Table 9. Critical Security Parameter Access by Service**

| Service Name | IPSec Encryption Key | TLS Encryption Key | Access Point Encryption Key | IPSec Integrity Key | TLS Integrity Key | Access Point Integrity Key | DRNG Key for X9.31 | DRNG Key for 186-2 | IPSec Private Key (ICO) | IPSec Private Key (User) | TLS Private Key | ECO Pass-word | IPSec Pre-Shared Key | TLS Pre-Master Secret | Diffie-Hellman Private Key | IKE Encryption Key | IKE Integrity Key |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Module Self-Test & Initialize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Init | Init | | | | | | | Zeroize | Zeroize | Zeroize |
| Module Show Status | | | | | | | | | | | | | | | | | |
| Radio Resource Management | | | | | | | | | | | | | | | | | |
| Zeroize CSP | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize | Reset | Zeroize | Zeroize | Zeroize | Zeroize | Zeroize |
| Change ECO Password | | | | | | | | | | | | Write | | | | | |
| Generate RSA Key Pair | | | | | | | | Update | Create | Create | Create | | | | | | |
| Load RSA Key & Cert | | | | | | | | | Create | Create | Create | | | | | | |
| Update Firmware | | | | | | | | | | | | | | | | | |
| Set IPSec/IKE Pre-Share Key | | | | | | | | | | | | | Write | | | | |
| IPSec/IKE Session Establishment for ICO role | Write | | | Write | | | Update | | Read | Read | | | Read | | Write | Write | Write |

 

| Service Name | IPSec Encryption Key | TLS Encryption Key | Access Point Encryption Key | IPSec Integrity Key | TLS Integrity Key | Access Point Integrity Key | DRNG Key for X9.31 | DRNG Key for 186-2 | IPSec Private Key (ICO) | IPSec Private Key (User) | TLS Private Key | ECO Pass-word | IPSec Pre-Shared Key | TLS Pre-Master Secret | Diffie-Hellman Private Key | IKE Encryption Key | IKE Integrity Key |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPSec Session Data Transfer for ICO role | Read | | | Read | | | Update | | | | | | | | | | |
| Transfer IPSec session for User role | Read & Write | | | Read | | | Update | | Read | | | | | | | | |
| IPSec/IKE Session Establishment for User role | Write | | | Write | | | Update | | | Read | | | Read | | Write | Write | Write |
| IPSec Session Data Transfer for User role | Read | | | Read | | | Update | | | Read | | | | | | | |
| TLS Session Establishment for ECO role | | Write | | | Write | | | Update | | | Read | | | Write, Read | | | |
| TLS Session Data Transfer for ECO role | | Read | | | Read | | | | | | Update | | | | | | |
| LWAPP Session Establishment for ICO role | | | Create | | | Create | | Update | Read | | | | | | | | |
| LWAPP Session Data Transfer for ICO role | | | Read | | | Read | | Update | | | | | | | | | |

Notice that one service (Module Show Status) does not access any Critical Security Parameters.

Note that zeroizing the ECO Password means setting it to the factory default password.

 

# 10 CSP by Service and Role Access Policy

The following table presents the policy that controls which CSP are accessed by each service when that service is performed by the each role.

**Table 10. Matrix of Role, Service, CSP Access**

| Role | | | Service | CSP Access Operation |
|---|---|---|---|---|
| User | ICO | ECO | | |
| X | X | X | Module Self-Test & Initialize | Zeroize session keys (TDES, AES, HMAC-SHA-1), Initialize DRNG State. |
| X | X | X | Module Show Status | None. |
| X | X | X | Radio Resource Management | None. |
| | | X | Zeroize CSP | Zeroize all CSP. |
| | | X | Change ECO Password | Write ECO Password. |
| | | X | Generate RSA Key Pair | Update DRNG State, Write RSA Public Key and Write RSA Private Key. |
| | | X | Load RSA Key & Cert | Write RSA Public Key and Write RSA Private Key. |
| | | X | Update Firmware | Read RSA Public Key. |
| | | X | Set IPSec/IKE Pre-Share Key | Write IPSec Pre-Share Key. |
| | X | | IPSec/IKE Session Establishment for ICO role | Write TDES or AES key, Write HMAC-SHA-1 key, Update DRNG State, Read RSA Public Key, Read RSA Private Key, Read IPSec Pre-Share Key, and write IKE keys for encryption and integrity and Diffie-Hellman. |
| | X | | IPSec Session Data Transfer for ICO role | Read TDES or AES key, Read HMAC-SHA-1 key and Update DRNG State (IV generation). |
| | X | | Transfer IPSec session for User role | Write TDES or AES key, Write HMAC-SHA-1 key. |
| X | | | IPSec/IKE Session Establishment for User role | Write TDES or AES key, Write HMAC-SHA-1 key, Update DRNG State, Read RSA Public Key, Read RSA Private Key, Read IPSec Pre-Share Key write TDES and AES keys for IKE and write IKE keys for encryption and integrity and Diffie-Hellman. |
| X | | | IPSec Session Data Transfer for User role | Read TDES or AES key, Read HMAC-SHA-1 key and Update DRNG State (IV generation). |
| | | X | TLS Session Establishment for ECO role | Write TDES or AES key, Write HMAC-SHA-1 key, Update DRNG State, Read RSA Public Key, Read RSA Private Key, and Write (or Read for TLS Reconnect) the TLS Pre-Master Secret. |
| | | X | TLS Session Data Transfer for ECO role | Read TDES or AES key, Read HMAC-SHA-1 key and Update DRNG State (IV generation). |

 

| Role | | | Service | CSP Access Operation |
|---|---|---|---|---|
| **User** | **ICO** | **ECO** | | |
| | X | | LWAPP Session Establishment for ICO role | Write AES key, Write HMAC-SHA-1 key and Update DRNG State. |
| | X | | LWAPP Session Data Transfer for ICO role | Read AES key, Read HMAC-SHA-1 key, Update DRNG State (IV generation). |

 

# 11 Physical Security Policy

The physical security of the module is designed to meet the requirements of FIPS-140-2 Level 2.

The physical boundary of the cryptographic module is the same as the physical boundary of the device. The cryptographic boundary of the module is the hard metal enclosure.

The module does not include a maintenance mode, so the FIPS-140-2 maintenance mode requirements do not apply.

The following table describes the recommended inspection/testing regime.

**Table 11. Inspection/Testing of Physical Security Mechanisms**

| Physical Security Mechanism | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|---|---|---|
| Tamper-evident seals. | Once per month. | Examine seals for signs of removal, replacement, or tearing. Two seal are located on the back panel in the center and right side. One seal is on the top in the center near the front. |
| Hard opaque production grade enclosure. | Once per month. | Examine enclosure for signs of any new openings having been cut into the device. |

## *11.1 Multi-Chip Standalone*

The ACM module is being validated as a "multi-chip standalone" cryptographic module. The physical boundary of the ACM cryptographic module is the same as the physical boundary of the device.

 

## *11.2 Physical Interfaces*

The ACM module has the following physical interface ports.

**Table 12. Physical Interface Ports**

| Interface Name | Interface Type | Interface Description |
|---|---|---|
| Power Receptacle | Power | Receptacle for 110 VAC power cord. |
| Power LED | Status | Green LED indicated that the device is powered on. |
| Error LED | Status | Red LED indicating the module status. When the device is turned on and the self-tests are running the LED is red. If the self-tests pass, the LED turns black. If the module enters the FIPS Error state, the LED becomes red. |
| GigaBit Activity LED | Status | Green LED flashes to indicate activity on the GigaBit port. |
| DB-9 Management Serial Port | Status | This DB9 connector provides terminal access to the module's command line interface. In the FIPS-140 build of the firmware only status commands are available. |
| RJ45 Management Network Port | Data I/O, Status, Control | This RJ45 connector provides 100 Mbps network port for the management interface. The ECO uses this port to establish a TLS secured connection to the module. |
| Gigabit Distribution Network Port | Data I/O, Control | This optional port provides fiber optic or copper wire access to a high-speed network that carries plaintext to and from the module, and carries cryptographically secured (IPSec/IKE) data and control information for communicating with other ACM modules. |
| 100 Mbps Distribution Network Port | Data I/O, Control | When the Gigabit port is not used, then one of the RJ45 ports (other than the Management Port) can be configured to be the port for distributing data to the wired network. All other RJ45 ports are used to connect to Access Point devices. |
| RJ45 Access Point Ports | Data I/O, Control | Twelve or twenty-four RJ45 connectors provide 10/100 Mbs Ethernet access to a network. These ports carry cryptographically secured data and control information. |
| RJ45 Status LEDs | Status | Each RJ45 connector has two green LEDs. The left one is on when a device is connected properly to the port, and the other LED blinks when data is transmitted or received. |

All models of the ACM have the physical interface ports listed above, except for the optional Gigabit Distribution Network Port; however, the number of RJ45 Access Point Ports does vary between models. See Section 4.5 for a listing of the ports that are present on each model of the ACM.

As explained in Section 4.5, the module can have two different internal power supplies, though they have the same Power Receptacle interface port.

 

# 12 Operational Environment Policy

The module operates in a *limited operational environment*. The module only supports the loading of digitally signed code using RSA. Any loading of unvalidated code invalidates the FIPS 140-2 validation. The integrity of the firmware is checked on power-on using SHA-1 as explained in Section 15.3. This applies to all firmware in the module.

Given the limited operational environment, the requirements of FIPS-140-2 section 4.6.1 (operating system requirements) do not apply.

# 13 Cryptographic Key Management Policy

This section describes the cryptographic key management policies of the module.

As detailed below, the module does not allow for the input of plaintext CSP, and it does not output plaintext CSP.

**Deterministic Random Number Generation**

The module uses two FIPS approved Deterministic Random Number Generators (DRNG). The algorithms are specified in ANSI X9.31 Appendix A, and FIPS-186-2 Appendix 3.1 (based on SHA-1). The seed keys for these are generated internally.

**Key Establishment**

The module supports commercially available establishment methods for IPSec/IKE, LWAPP, and TLS. The cipher suites for these protocols are chosen to comply with FIPS-140-2. These methods establish symmetric keys for TDES, HMAC-SHA-1 and 128-bit keys for AES.

The effective strength of the established keys is 80 bits as indicated in Section 4.4.

**Key Zeroization**

The non-persistent session CSPs are zeroized upon power cycle.

The External Crypto Officer can invoke a service that zeroizes the persistent CSP (e.g., the RSA private key for TLS). This command also resets the ECO password to its factory default. This command does not zeroize any of the non-persistent session keys.

To fully zeroize the CSP on the module, the ECO must perform the steps below.

1. Connect to the module via a TLS session.

2. Authenticate using a password.

3. Invoke the command that zeroizes persistent keys and CSPs.

4. Terminate the TLS session.

5. Power-cycle the module.

The zeroization is performed by a single overwrite of the memory location that holds a key or other CSP value.

 

# 14 Electromagnetic Interference and Compatibility

As required by FIPS-140-2 at Level 2, the module conforms to the EMI/EMC requirements specified by 47 Code Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for commercial use). The device is labeled accordance with FCC regulations.

# 15 Description of Self-Tests

This section describes the Power-On Self-Tests and the Conditional Self-Tests supported by the module. The module does not support any critical functions, so there are no critical function tests.

The module supports a service called "Module Self-Test & Initialize" that does the following. It is invoked by powering on the module and does not require any operator intervention.

1. Performs the power-on self-test. If any fail, enter the FIPS Error state and stop.
2. Zeroizes all Critical Security Parameters stored in RAM (e.g., session keys) and clears all remembered authentication results, and
3. Initializes the module.

This sequence ensures that the module will not perform any input or output while the self-tests are being performed.

## *15.1 Power-On Self-Tests*

The following table lists the self-tests that are performed by the module.

**Table 13. Description of Power-Up Self-Tests**

| Test Name |
|---|
| Firmware Integrity Test |
| DRNG KAT |
| HMAC-SHA-1 KAT |
| SHA-1 KAT |
| TDES-CBC KAT |
| AES-128-CBC KAT |
| RSA Sign KAT |
| RSA Verify KAT |
| RSA Wrap Pairwise Consistency Test<br>RSA Unwrap Pairwise Consistency Test |

 

## 15.2 Conditional Self-Tests

The following table lists the conditional self-tests that are performed by the module. The continuous RNG tests are performed on all RNG including the non-deterministic RNG that is used to seed the FIPS approved DRNG.

**Table 14. Description of Conditional Self-Tests**

| Test Name |
|---|
| Continuous Random Number Test for FIPS 186-2 DRNG |
| Continuous Random Number Test for ANSI X9.31 DRNG |
| Continuous Random Number Test for HiFn Non-Deterministic RNG |
| Pair-wise Consistency Test |
| Firmware Load Test |

## 15.3 Firmware Integrity Test

When power is applied to the module, the module performs a 160-bit error detection code (EDC) test, which exceeds the 16-bit test required by FIPS-140-2.

# 16 Mitigation of Other Attacks Policy

The cryptographic module only provides mitigation against attacks for which testable security requirements were specified for FIPS-140-2 Level 2. It does not mitigate attacks outside the scope of FIPS 140-2.

**Table 15. Mitigation of Other Attacks**

| Other Attacks | Mitigation Mechanism | Specific Limitations |
|---|---|---|
| N/A | N/A | N/A |

 

# 17 Glossary

The following paragraphs define the acronyms used in this document.

**ACM**. Airespace Cryptographic Module.

**AES**. Advanced Encryption Standard. See [FIPS-197].

**DES**. Data Encryption Standard. See [FIPS-46-3].

**DH**. Diffie-Hellman public key algorithm.

**DRNG**. Deterministic Random Number Generator.

**ECO**. External Crypto Officer role.

**EDC**. Error Detection Code.

**FIPS**. Federal Information Processing Standard of NIST.

**HMAC-SHA-1**. Hash-based Message Authentication Code based on SHA-1. See [FIPS-198].

**ICO**. Inter-module Crypto Officer role.

**IETF**. Internet Engineering Task Force standards group.

**IPSec/IKE**. IP Security and Internet Key Exchange protocols.

**ISO**. International Standards Organization.

**LWAPP**. Light Weight Access Point Protocol.

**MD5**. Message Digest algorithm 5 by Professor Ronald Rivest.

**NIST**. National Institute of Standards and Technologies.

**RC4**. Rivest Cipher algorithm 4 by Professor Ronald Rivest.

**SHA-1**. Secure Hash Algorithm revision 1. See [FIPS-180-2].

**SSL**. Secure Socket Layer protocol. See [TLS].

**TDES**. Triple DES. See [FIPS-43-3].

**TLS**. Transport Layer Security protocol. See [TLS].

**X9**. ANSI/ISO financial standards group.

**X9.31**. A key management standard of the X9 group.

**X9.509**. A digital certificate standard of the X9 group.

 

# 18 References

The following documents provide additional reference material.

[FIPS-46-3] "Data Encryption Standard (DES)" Version 3, October 25, 1999. FIPS-46-3. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-140-2] "Security Requirements for Cryptographic Modules" Version 2, May 25, 2001. FIPS-140-2. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FIPS-140-IG] "Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program" December 4, 2001.

[FIPS-180-2] "Secure Hash Standard" Version 2. August 1, 2002. FIPS-180-2. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[FIPS-186-2] "Digital Signature Standard (DSS)" Version 2, January 27, 2000. FIPS-186-2. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

[FIPS-197] "Advanced Encryption Standard (AES)" November 26, 2001. FIPS-197. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS-198] "The Keyed-Hash Message Authentication Code (HMAC)" March 6, 2002. File updated April 8, 2002. FIPS-197. http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

[IPSec] "Security Architecture for the Internet Protocol." By S. Kent, R. Atkinson. November 1998. RFC 2401. See: http://www.ietf.org/rfc/rfc2401.txt

[LWAPP] "Light Weight Access Point Protocol (LWAPP)" By P. Calhoun, B. O'Hara, S. Kelly, R. Suri, D. Funato, M. Vakulenko. June 28, 2003. See: http://www.ietf.org/internet-drafts/draft-calhoun-seamoby-lwapp-03.txt

[NIST-KMG] "Key Management Guideline" Draft of June 3, 2002. NIST. See: http://csrc.nist.gov/encryption/kms/guideline-1.pdf

[Schneier] Applied Cryptography by Bruce Schneier. Second Edition. 1996. John Wiley & Sons. ISBN 0-471-11709-9. See: http://www.amazon.com/exec/obidos/ASIN/0471117099/

[TLS] "The TLS Protocol Version 1.0." by T. Dierks and C. Allen. January 1999. RFC 2246. See: http://www.ietf.org/rfc/rfc2246.txt

 