# FIPS 140-2 Non-Proprietary Security Policy

Infraguard Processor Module

Advantor Systems, A Vectrus Company
12612 Challenger Pkwy, Suite 300
Orlando, FL 32826
USA

June 22, 2021

Revision 1.19

# Table of Contents

# FIPS 140-2 Non-Proprietary Security Policy

Infraguard Processor Module

## 1. Introduction

The Infraguard Processor Module (IPM) is a multi-chip embedded encryption module coated with an opaque, tamper evident material. The cryptographic boundary is the entire module. The IPM is a plug-in module that is intended to meet FIPS 140-2, Security level 2 requirements.

| FIPS 140-2 Security Level Summary | | |
|---|---|---|
| Section | Title | Level |
| 1 | Cryptographic Module Specification | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 2 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key Management | 2 |
| 8 | EMI/EMC | 2 |
| 9 | Self-Tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

The IPM is used to provide secure communications for Advantor Systems' physical security systems, communicating over either LAN or telephone line.

The module may be incorporated into multiple products, such as alarm panels (i.e. Infraguard II) and alarm receiving equipment (i.e. IMI-NET v2).

The IMI-NET v2 receives alarm and status event data from up to 32 Infraguard II alarm panels connected via dedicated or dial-up telephone lines. Serial (modem) communications are encrypted with the IPM's Codeload application. Unencrypted data from the panel or receiver application is passed to and from Codeload using 'named pipes'. The IPM also allows the connection with a firewall device, such as the Cisco 5506, via IPSec, to provide secure communications over LAN. The IPMs and the firewall use preshared keys for encryption. All keys are managed with the Cryptoadmin application, including the serial devices' peer authentication keys and the strongSwan configuration settings.

### *1.1. Purpose*

This document covers the secure operation of the IPM including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner.

### *1.2. Glossary*

| Term/Acronym | Description |
|---|---|
| IPM | Infraguard Processor Module |
| CO | Cryptographic-officer or Crypto-officer |
| ID | Identification number |

| | |
|---|---|
| strongSwan | VPN client for Cisco ASA 5506 and like firewall devices |

# 2. Ports and Interfaces

Below is a mapping of the physical ports of this module to the logical interfaces.

| Logical Interface | Physical Port |
|---|---|
| Data Input | 240 pin DIMM connector<br>3,4 Ethernet RX<br>173 Modem RX<br>203-210 (I/O data bus) |
| Data Output | 240 pin DIMM connector<br>1,2 Ethernet TX<br>172 Modem TX<br>203-210 (I/O data bus) |
| Control Input | 240 pin DIMM connector<br>141 RS-232 TX (admin)<br>142 RS-232 RX (admin) |
| Status Output | 240 pin DIMM connector<br>7 Ethernet link<br>8 Ethernet speed<br>9 Ethernet active<br>60 status LED<br>61 status LED |
| Power Interface | 240 pin DIMM connector<br>GND 6,15,17,19,24,39,40,129,130,163,164<br>GND 166,168,170,76,77,101,102,196,198<br>GND 200,202,226,228,230,232<br>3.3 VDC 16,18,37,39,165,167,169,192,193<br>3.3 VDC 197,199,201,227,229,231<br>5 VDC 113,114<br>1.2 VDC 161 |

# 3. Roles, Services, and Authentication

The IPM provides three different roles and a set of services particular to each of the roles. The three roles are 'crypto-officer', 'user' and 'maintenance'. The IPM will authenticate a crypto-officer's identity by verifying login name and password. All encryption keys, including preshared keys for devices, and the VPN client configuration settings, are managed by Crypto-officers. The 'user' role is not authenticated and has no access to the IPM security relevant data items (SRDI). When the IPM is in the 'operation mode', or 'encrypt / decrypt data state', user data is supplied to the IPM for encryption / decryption. The maintenance role is for updating or repairing the IPM module by the manufacturer.

## *3.1. Roles*

*User Role*

Users of the IPM, to secure communications over an untrusted network or modem channel, are not authenticated by the IPM. Users have no access to, or control over, the IPM's security functions or SRDIs. Users supply unencrypted data to the IPM over the trusted interface for secure communications over an untrusted interface. The user's sole-service is to communicate with a remote IPM.

*Crypto-Officer Role*

The Crypto-officer has access to the IPM's administrative commands. A Crypto-officer must initialize a new IPM upon receipt and then can create an administrator, delete an administrator, or set a key for a specified panel number. Once authenticated, the Crypto-officer can perform any of the following services (commands):

user add; login name (adds an administrator, prompts for password, masks entry, confirms by duplicate entry)
user delete; login name
user unlock; (login name)
user change-password; (prompts for key, masks entry, confirms by duplicate entry)
set hostname; (clear with empty entry)
set local-ip; IPv4 address
set local-subnet; IPv4 address
set local-gateway; IPv4 address
set remote-syslog-ip; IPv4 address
set server-ip; IPv4 address
set server-backup-ip; IPv4 address
set local-DNS; IPv4 address
set dhcp; (on/off)
set syslog-info; (on/off) turn on additional logging
set transition_mode; (on/off)
show console-timeout;
show panels; (device IDs that are assigned a key, and key size)
show network; (displays network settings)
show users; (displays administrators' login names)
show ipsec-conf; (IPSec parameters except secret)
show tunnel-status; Show VPN status (up/down)
show syslog; show current log
show versions; show the versions of the Advantor proprietary FIPS applications
show transition_mode; if "on" panel is NOT operating in FIPS 140-2 compliance
crypto key; panel ID (prompts for key, masks entry, confirms by duplicate entry)
crypto ipsec-conf; set connection name
crypto ipsec-conf-clear; clear ipsec configuration
crypto ipsec-secrets; (prompts for key, masks entry, confirms by duplicate entry)
crypto ipsec-secrets-clear; clear ipsec secret
crypto vpn-mode; set to IPSEC or NONE
maintenance; enter maintenance mode
console-timout; set timout in seconds
run-self-test;
zeroise;
reboot;

*Maintenance Role*

A Crypto-officer may command the module to enter maintenance mode (see above). When the module is placed in maintenance mode, it is zeroized and all IPM cryptographic functions are disabled, including the administration console. When the module is restarted from maintenance mode, the maintenance mode will automatically be cleared, the module will be zeroized, and the module will be rebooted for standard operation. As the maintenance role, an operator has access to the Zeroize, SSH Enabled and Update/Repair services. SSH is only accessed for in house maintenance and repair

work. The maintenance role has no separate authentication aside from the crypto-officer commanding the module to enter maintenance mode. The maintenance role will only either re-manufacture or replace the module.

### *3.2. Authentication Mechanisms and Strength*

The IPM authenticates crypto-officers by login name and password. The IPM enforces password strength, requiring minimum 16 characters in length, at least one number, one symbol from the set of 30 characters {~!@#$%^&*()_+=-\|[]{};:'",.<>?}, one lower case character, and one upper case character. This yields a probability of success or false acceptance to an estimated less than 4.463818*10^30 for a single attempt. Attempts are limited to 6 after which the module locks out the user. The probability in 6 attempts is approximately 1 in $5x10^{30}$. In all cases, password data entry is displayed with an asterisk "*" during entry, and no functions are provided to display passwords.

*Login Authentication*

Crypto-officers authenticate to the IPM using a login and password, a crypto-officer must log in to the Crypto-officer application using the RS-232 port. If the password is entered incorrectly 6 times, without a valid login, the login will be disabled until unlocked by another crypto-officer, or the module is zeroized.

*Operation Mode*

In the 'operation mode', user data is sent to, and received from, the IPM on the trusted interface (named pipes) and encrypted data is sent to, and received from, either another IPM, over a serial communications channel, such as a modem channel. or a network device, such as a firewall, using IPSec communications. The IPSec PSK is a string of 16 randomly generated alphanumeric characters (62^16 = 4.7672402e+28). VPN timeout of 30 minutes, and operator console timeout of 20 seconds.

# 4. Secure Operation and Security Rules

In order to operate the Infraguard Processing Module securely, the operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules required.

### *4.1. Security Rules*

The security rules enforced by the IPM result from the security requirements of FIPS 140-2.

*FIPS 140-2 Security Rules*

The following are security rules that stem from the requirements of FIPS PUB 140-2. The module enforces these requirements when initialized into FIPS level 2 Mode.

1. When initialized to operate in FIPS level 2 Mode, the IPM only uses FIPS-approved or FIPS allowed cryptographic algorithms.
2. The IPM employs a DRBG compliant with Special Publication 800-90Arev1.
3. The IPM provides authentication of operators by verifying the operator's login name and password.
4. The IPM provides the Crypto-officer the capability the zeroize the plaintext critical security parameters contained within the IPM including the keys for serial communications and VPN network communications..
5. In no case will the IPM output any security relevant data items (SRDI), including device keys for serial communications, VPN keys for network communications, crypto-officer passwords, etc.

6. Data entry for all SRDI keys and passwords is echoed with a mask * character.
7. Keys must be entered from a non-networked GPC (General Purpose Computer)

### *4.2. Physical Security Rules*

The owner of the IPM must periodically inspect the physical case of the IPM to ensure that no attacker has attempted to tamper the IPM. Signs of tampering include:

Deformation, scratches, or scrapes in the opaque, hard epoxy covering the Module.

*Operator Actions*

The operator shall contact Advantor Support if evidence of tampering is found.

### *4.3. Secure Operation Initialization Rules*

The IPM generates at least 256 bits of entropy before generating keys (SP 800-90B) and provides the following approved algorithms in FIPS mode:

| Algorithms Supported | Modes/Mod sizes | Standard | Algorithm Certificate | Usage |
|---|---|---|---|---|
| KTS | AES-CBC (256-bit keys) and HMAC-SHA256 | SP 800-38F/FIPS 140-2 IG D.9 | AES Cert. #A931 and HMAC Cert. #A931 | Key Transport |
| AES CBC | 256-bit | FIPS 197<br>SP 800-38A | AES Cert. #A931 | Communication encryption |
| HMAC | SHA-1<br>SHA-256<br>SHA-512 | FIPS 198-1 | HMAC Cert. #A931 | Signature for dynamic keys |
| DRBG | HMAC SHA256 | SP 800-90Arev1 | #A931 | Seed encryption and producing dynamic keys |
| SHS | SHA256 | FIPS 180-4 | #A931 | Verify code |
| KAS | dhEphem, MODP-2048 | SP 800-56Arev3<br>SP 800-56Crev1 | KAS-SSC Cert. #A932<br>CVL Cert. #A932 | IPSec Key establishment methodology provides 112 bits of encryption strength. |
| CVL | IKEv2 KDF[1] | SP 800-135 | #A932 | IKEv2 KDF |
| CKG | Asymmetric keys generated according to Section 5.2.<br>Symmetric keys generated according to Section 6.1 | SP 800-133rev2 | Vendor Affirmed | Key generation |
| SafePrime KeyGen | 2048-bit | SP 800-135<br>SP 800-56Arev3 | #A931 | Diffie-Hellman |
| ENT (NP) | | SP 800-90B | | Entropy Source |

[1] No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

Not all algorithms/modes tested by the ACVP are utilized by the module.

No non-approved algorithms are supported in either approved or non-approved modes

Because FIPS 140-2 prohibits the use of non-FIPS approved algorithms while operating in a FIPS compliant manner, the Crypto-officer should adhere to the following rules to initialize a new IPM to ensure FIPS level 2-compliance:

1. Power-up the IPM
2. When the IPM enters the Uninitialized state, the operator should authenticate the IPM using the factory default login (administrator, advantor).
3. Before any crypto functions may be invoked, the operator must first change the default password [minimum 16 character password with at least one lower case character, upper case character, number and symbol].
4. After changing password, the operator should add additional crypto-officer logins, as required, using the ”add user” command. The operator should specify the following command parameters:
   Login name
   Login password: [minimum 16 character password with at least one lower case character, upper case character, number and symbol]
   Note: Maximum login tries are set to 6. After lockout, another Crypto-officer must log in to clear.
   Preshared key entry: device ID followed by key (device key entry is masked, and must be entered twice for confirmation)
   strongSwan parameters:
   1. IPSec connection ID.
   2. IPSec Secret, (masked during entry, and must be entered twice for confirmation).
5. Authenticate as the newly created Crypto-officer by logging in with login name and password.
6. Create any additional login names and passwords for IPM operators. They can change their password after login.

When initialized in this fashion, the IPM will only use FIPS-approved algorithms. Note that any operator can determine the state of an IPM at any time by requesting the “show status” command, which will return the initialized state of the IPM as FIPS or FIPS_FAIL.

# 5. Definition of SRDIs Modes of Access

This section specifies the IPM's Security Relevant Data Items as well as the access control policy enforced by the IPM.

### *5.1. Cryptographic Keys, HMAC Keys, CSPs, and SRDIs*

While operating in a level 2 FIPS-compliant manner, the IPM contains the following security relevant data items:

| Key/CSP | Description | Generation/Entry | Storage / Zeroization |
|---|---|---|---|
| Firmware Integrity Key | A 32-byte key embedded within the IPM's firmware image. This key is used to verify the firmware integrity code attached to a new firmware image using HMAC SHA512 . | The value is part of the firmware image and not generated or entered. | The key is stored in the firmware image in plaintext in flash storage.<br><br>The key is not zeroized. |
| Panel keys | Panel and signature keys are used for encrypting and decrypting temporary 'session' keys. The panel keys 256-bit AES pre-shared keys and the signature keys are SHA-256 HMAC. A separate pair of keys is entered for each "panel ID". Up to 10,000 keys may be entered for the IMI-NET v2. | Panel and signature keys are externally generated and entered in plain text via the serial interface by crypto-officer. | Panel keys and signature keys are stored in plaintext in flash storage.<br><br>Zeroization: The panel and signature key store file is deleted and zeroed during zeroization. |

| Key/CSP | Description | Generation/Entry | Storage / Zeroization |
|---|---|---|---|
| IMI-NET Session Keys | Session keys are 256-bit AES keys.<br><br>After the temporary session key is created, it is AES encrypted using the panel key, signed with HMAC-256 and transmitted to the connecting Infraguard II device. | The session key is generated using unmodified output from the approved DRBG.<br><br>The session key can be output in encrypted form using the panel key and signature key. | The session key is stored, in plain text, in volatile memory and is not persistent.<br><br>The session keys and HMAC key are set to “0” when the module is zeroized. |
| VPN configuration file | VPN is used by the IPM module for encrypting ‘user application’ communications traffic, over a TCP/IP network. | The VPN connection ID is manually distributed as is the VPN preshared key. Both are entered into the module by the crypto-officer in plaintext. | The connection ID is stored in plaintext within the flash storage in the ipsec.conf file. The preshared key is stored in plaintext within the flash storage in the ipsec.secrets file.<br><br>The secrets file is deleted when the module is zeroized. |
| Crypto-officer Login Passwords | Crypto-officer logins and passwords are stored in an ‘admins’ file, in Flash memory. This file has ‘root only’ access. The password is used for authenticating crypto-officer logins. | Passwords are entered manually by crypto-officer in plaintext, generated by means at the discretion of the crypto-officer. | Passwords are stored in plaintext flash storage.<br><br>The administrator login / password file “admins.txt” is deleted when the module is zeroized. |
| Diffie-Hellman Public/Private Primes | 2048-bit prime values used for key establishment as part of IKE | The values are generated using a prime generation method that uses unmodified output from the approved DRBG. | The value is ephemerally stored in RAM and can be zeroized by power cycling the module. |
| KAS-FFC Shared Secret | 2048-bit shared secret computed from Diffie-Hellman Public/Private primes and input into the IKEv2 KDF | This value is computed from the local module’s Diffie-Hellman Private Prime and peer Public Prime | The value is ephemerally stored in RAM and can be zeroized by power cycling the module. |
| IKEv2 Session Keys | The values are used to institute communications as part of IPSec | AES256/HMAC-SHA1 derived from IKEv2 KDF | The value is ephemerally stored |

| Key/CSP | Description | Generation/Entry | Storage / Zeroization |
|---|---|---|---|
| | | | in RAM and zeroized during power cycle. |
| IPSec Session Keys | The values are used to encrypt communications over the network. | AES256/HMAC-SHA1keys | The value is ephemerally stored in RAM and zeroized during power cycle |
| DRBG Seed | The value is used to initialize the approved DRBG. | The value is generated using the system entropy source. | The value is ephemerally stored in RAM and zeroized during power cycle. |
| DRBG State | A value (V) of seedlen bits that is updated during each call to the DRBG. A key (key) is generated by the hash function from the seed. | Values used to create a new output of bits, updated each time output is generated. | V and key are ephemerally stored in RAM and can be zeroized by power cycling the module. |
| Entropy Input String | String of 384 random bits that produces the initial seed, along with periodic re-seeding. | Entropy produced by entropy source | Entropy string stored in RAM and is zeroized during power cycle. |

### *5.2. Access Control Policy*

The IPM allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the IPM in a given role performing a specific operation. The permissions are categorized as a set of four separate permissions: read (r), write (w), execute (x), zeroize (z). If no permission is listed, then an operator outside the IPM has no access to the SRDI.

| Advantor Infraguard Processing Module<br><br>Cryptographic Keys, HMAC Keys, CSPs, and SRDIs | | Panel Keys | Session Keys | Crypto-officer Passwords | VPN configuration files | Firmware Integrity Key | Diffie-Hellman Public/Private Primes | IKEv2 Session Keys | IPSec Session Keys | DRBG Seed | DRBG Seed Key | Entropy Input String |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Role | | | | | | | | | | | | |
| User role | | | | | | | | | | | | |
| Communicate with remote IPM | | x | wxz | | | | wxz | wxz | wxz | x | x | |
| Crypto-officer Role | | | | | | | | | | | | |
| user add | | | | w | | | | | | | | |
| user delete | | | | w | | | | | | | | |
| user unlock | | | | w | | | | | | | | |
| user change-password | | | | w | | | | | | | | |
| show users | | | | r | | | | | | | | |
| crypto key | | w | | | | | | | | | | |
| show ipsec-conf | | | | | r | | | | | | | |
| crypto ipsec-conf | | | | | w | | | | | | | |
| crypto ipsec-conf-clear | | | | | w | | | | | | | |
| crypto ipsec-secrets | | | | | w | | | | | | | |
| crypto ipsec-secrets-clear | | | | | w | | | | | | | |
| crypto vpn-mode | | | | | w | | | | | | | |
| show panels | | r | | | | | | | | | | |
| run-self-test | | | | | | x | | | | | | |
| zeroize | | z | z | z | z | | | | | z | z | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| set hostname | | | | | w | | | | | | | |
| set local-ip | | | | | w | | | | | | | |
| set local-subnet | | | | | w | | | | | | | |
| set local-gateway | | | | | w | | | | | | | |
| set remote-syslog-ip | | | | | w | | | | | | | |
| set server-ip | | | | | w | | | | | | | |
| set server-backup-ip | | | | | w | | | | | | | |
| set local-DNS | | | | | w | | | | | | | |
| set dhcp | | | | | w | | | | | | | |
| set syslog-info | | | | | w | | | | | | | |
| set transition_mode | | | w | | | | | | | | | |
| show console-timeout | | | | r | | | | | | | | |
| show network | | | | r | r | | | | | | | |
| show tunnel-status | | | | | | | | | | | | |
| show syslog | | | | | | | | | | | | |
| show versions | | | | | | | | | | | | |
| show transition_mode | | | | | | | | | | | | |
| maintenance | | z | z | z | z | | | | | z | z | |
| console-timout | | | | | | | | | | | | |
| reboot | | | z | | | | z | z | z | z | z | z |
| Maintenance Role (manufacturer) | | | | | | | | | | | | |
| SSH enabled | | | | | | | | | | | | |
| Zeroize | | z | z | z | z | | | | | z | z | |

## 6. Transition Mode

This module contains a Transition Mode.
Transition mode is a user-level function that may only be invoked on a panel device (e.g. Infraguard II). It is set with the configuration console by entering the command “set transition_mode on”. Similarly, it can be removed in the configuration console by entering the command “set transition_mode off”. The default setting, with no configuration command entered is “off”.

### *6.1. Transition Mode “ON”*

When transition mode is set to “ON”, the module is NOT in current FIPS 140-2 mode. This is indicated when the command “Show transition_mode” is entered in the configuration console. The purpose of transition mode is to allow a site to upgrade a

single panel without disrupting the operation of the rest of the system. It is only required when connecting a current FIPS 140-2 capable panel over a telephone line to an older IMI-NET (receiving device) which is not capable of current FIPS 140-2 operation.

### *6.2. Transition Mode "OFF"*

When transition mode is set to "OFF" the module is in full FIPS 140-2 mode. This is indicated when the command "Show transition_mode" is entered in the configuration console.

## 7. Self-Tests

### *7.1. Power Up Self-Tests*

This module contains the following Power Up Self-Tests:

AES 128 and AES 256 ECB and AES 128 CBC, Encrypt and Decrypt Known Answer Tests
HMAC (SHA-1, SHA-256, SHA-512) Known Answer Tests
DRBG Instantiate, Generate, Seed and Reseed Known Answer Tests
FFC Primitive Z 2048 bits Known Answer Test
Firmware Integrity Test (HMAC SHA-512)
IKEv2 KDF KAT
SP 800-90B Startup Health tests: Adaptive Proportion Test and Repetition Count Test

### *7.2. Conditional Self-Tests*

The module contains the following conditional self-tests

SP 800-90B Health tests for Entropy Source
- Adaptive Proportion Test
- Repetition Count Test

Continuous Random Bit Generation Test for the Deterministic Random Bit Generator
SP 800-56Arev3 conditional assurances

## 8. Mitigation of Other Attacks

This section is not applicable

## 9. Cryptographic Boundary

Operational Environment is a non-modifiable operational environment. The hardware cryptographic boundary is the entire IPM. The firmware boundary includes all portions that relate to communication outside of the module. This includes the entropy producing Jitterentropy, the auxiliary DRBG program urandom, the cryptographic library libgcrypt, the IPSec application strongswan, the FIPS 140-2 configuration application cryptoadmin and the communication program codeload. Specifically excluding from the firmware FIPS 140-2 boundary are the proprietary Advantor applications imi-net.elf and inf_fact.bin / inf_dld.bin. These applications consume decrypted data, produce data to be encrypted and receive status. They do not take part in any FIPS 140-2 related functions.

## 10. Revision Levels:

Hardware revision level: 5.16

Hardware Versions:

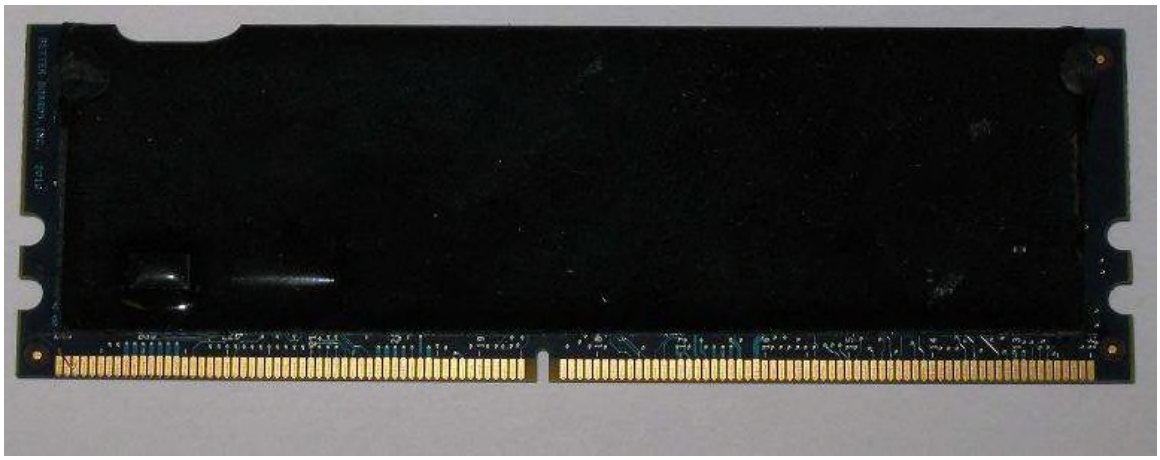
5.16 with components NAND MX30LF1G08AA-TI and SDRAM MT48H16M32LFB5-6 IT:C
5.16 with components NAND S34ML01G100TFI000 and SDRAM MT48H16M32LFB5-6 IT:C
5.16 with components NAND MT29F2G08ABAEAWP-AITX:E and SDRAM MT48H16M32LFB5-6 IT:C
5.16 with components NAND K9F1G08U0D-SIB0 and SDRAM MT48H16M32LFB5-6 IT:C
5.16 with components NAND MX30LF1G08AA-TI and SDRAM MT48H16M32LFB5-6 AAT:C
5.16 with components NAND S34ML01G100TFI000 and SDRAM MT48H16M32LFB5-6 AAT:C
5.16 with components NAND MT29F2G08ABAEAWP-AITX:E and SDRAM MT48H16M32LFB5-6 AAT:C
5.16 with components NAND K9F1G08U0D-SIB0 and SDRAM MT48H16M32LFB5-6 AAT:C

Firmware: version 2.3.0

### 10.1. FIPS 140-2 Versions *(contained within firmware version 2.3.0)*[2]

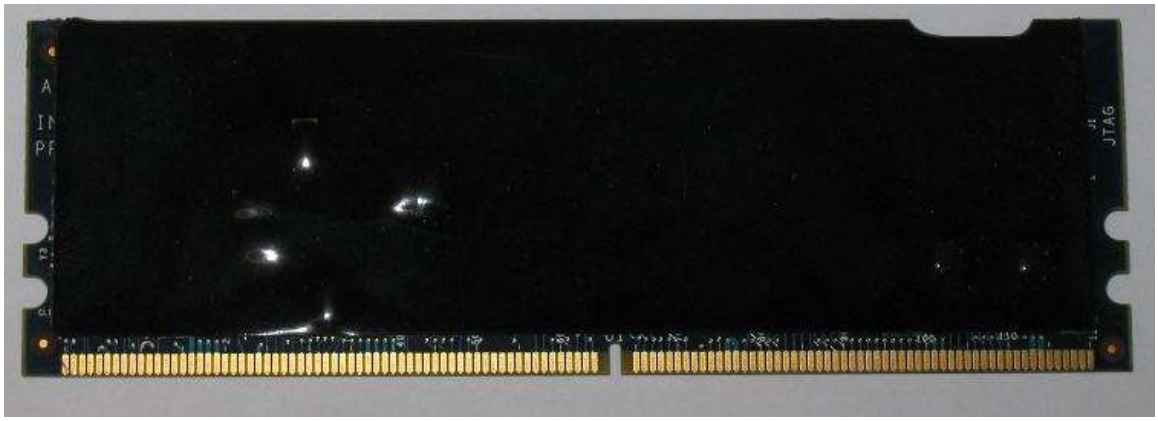
Jitterentropy: 2.2.0
libgcrypt: 1.8.4-advantor
Strongswan: 5.6.0-advantor
Codeload: 1.300
Cryptoadmin: 1.300
Urandom: 1.0

## 11. IPM Image - Front



[2] Firmware version infers hardware version

## 12. IPM Image - Back




## 13. Secure Delivery

The security of the IPM cannot be assured if the device is received from the factory with evidence of tampering. If the shipping packaging of the product, or the tamper evident coating on the IPM show signs of tampering, contact an Advantor Systems customer service representative.