AUTOSOL
Data in motion.

CryptoMod®

THE KEY TO
AUTOMATION SECURITY.

End Point Protection for Remote Field Devices,
Optimized for SCADA, Designed for IIoT.

# FIPS 140-2 Non Proprietary Security Policy
# Level 2
# Document Version 1.1.5

## *Table Of Contents*

## *List of Tables*



## *List of Figures*

# 1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the AUTOSOL CryptoMod, which for the duration of this document will be referred to as CryptoMod only. Below are the details of the product certified:

Hardware Version #: CM5705-D9
Firmware Version #: 1.0.51.FIPS
FIPS 140-2 Security Level: 2

## 1.1 Purpose

This document was prepared as Federal Information Processing Standard (FIPS) 140-2 validation process. The document describes how the CryptoMod meets the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. Target audience of this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-2 requirements.

## 1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

## 1.3 Notices

## 2. AUTOSOL CryptoMod

The CryptoMod (the module) is a multi-chip standalone module validated at FIPS 140-2 Security Level 2. Specifically, the module meets that following security levels for individual sections in FIPS 140-2 standard:

Table 1 - Security Level For Each FIPS 140-2 Section

| # | Section Title | Security 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 Assurances | 2 |
| **11** | Mitigation Of Other Attacks | N/A |
| **12** | Overall Level | 2 |

## 2.1 Cryptographic Module Specification

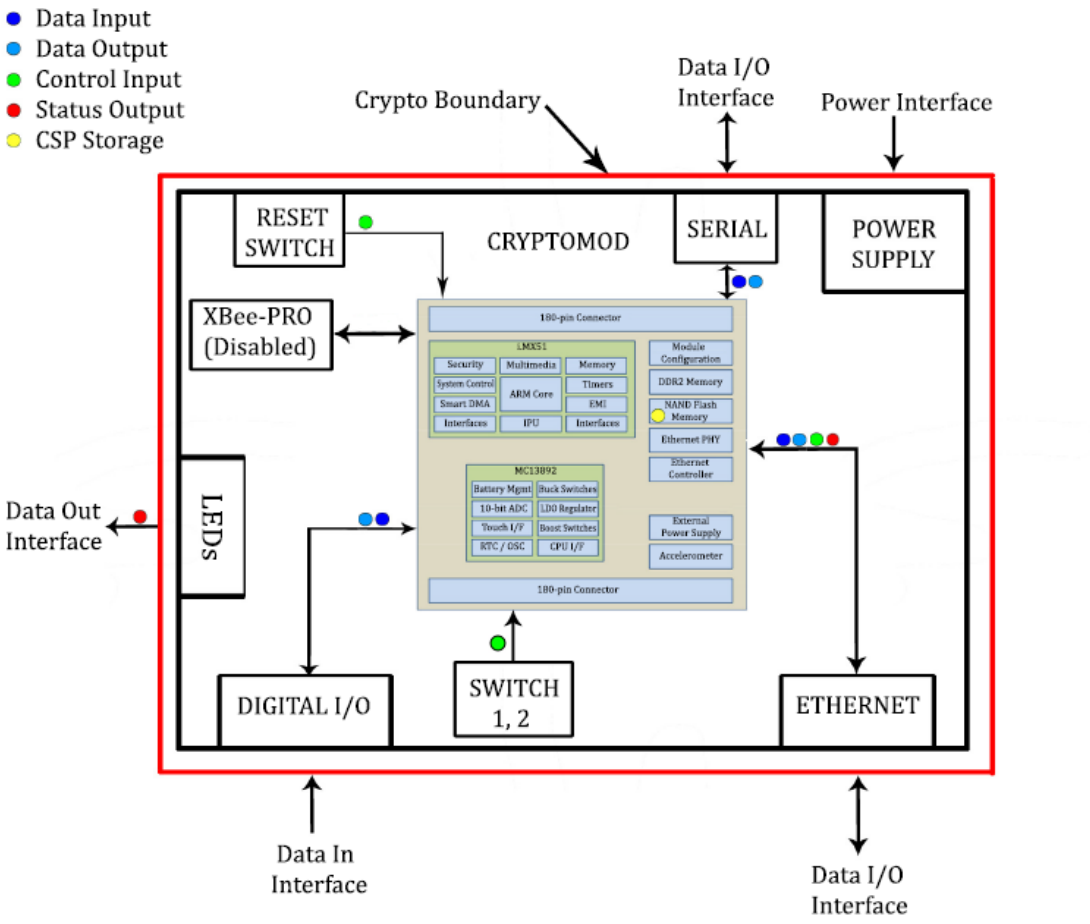
AUTOSOL's CryptoMod is an end-point security device designed to protect data exchanged between remote industrial field devices and a centralized SCADA host. Installed directly in front of the remote assets you want to protect, the CryptoMod encrypts network traffic for the entire length of an industrial network. The CryptoMod is device and protocol neutral, acting as an invisible secure pass through for network traffic. The CryptoMod provides authentication for controlling network access, integrity for data when it's in motion, and confidentiality for network traffic. The CryptoMod also offers physical intrusion detection to its enclosure. The CryptoMod carries a CSA Class 1 Div. 2 Hazardous Area Classification and functions as a terminal server, allowing it to fit any existing industrial network configuration without the need to re-configure the network. Since reliability is the foundation of safety, the CryptoMod has a hardware watchdog timer as well as the capability to be remotely configured, managed, and updated. Extensive logs with forwarding capabilities provide auditable files for detailed network monitoring. The CryptoMod provides network security as close to an industrial network's edges as possible in order to maintain data availability and, ultimately, process safety.

Figure 1 - The CryptoMod

### 2.1.1 Cryptographic Boundary

The cryptographic boundary is defined as being the physical enclosure of the CryptoMod. All of the functionality described in this publication is provided by components within this cryptographic boundary.

Figure 2 - CryptoMod Block Diagram



### 2.1.2 Modes Of Operation

After the Crypto-Officer has performed the initial configuration and setup described in Section 3 of this document, the module will be in its Approved mode of operation.

Table 2 - Supported Approved Algorithms

| CAVP Cert. # | Cryptographic Algorithm | Usage |
|---|---|---|
| **1255** | DRBG (NIST SP 800-90Arev1) | Functions: Hash DRBG Random Number Generation; Key generation. Size: 1, 256 and 384 bit. |
| **2257** | RSA (FIPS 186-4 | Functions: Digital Signature Generation/Verification and Asymmetric Key Generation. Size: 2048 and 3072 bit |
| **4140** | AES (NIST SP 800-38A) | Functions: Encryption/Decryption, Key Generation. Mode: CBC mode. Size: 128 and 256 bit |
| **3410** | SHA (FIPS 180-4) | Functions: Hashing. SHA Sizes: 1, 256 and 384 bit |
| **2713** | HMAC (FIPS 198-1) | Functions: Message Authentication. SHA Sizes: 1, 256 and 384 bit |
| **946** | CVL (NIST SP 800-135) | Functions: Key Derivation Function. TLS 1.2 |
| **Vendor Affirmed** | PBKDF2 (NIST SP 800-132) | Functions: Password Based Key Derivation Function. The vendor affirms compliance with SP 800-132, using option 1(a) in Section 5.4 |

The Cryptographic Module also provides the following non FIPS-approved but allowed algorithms:

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength.)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 bits of encryption strength.)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength.)
- NDRNG (for seeding the Approved DRBG)

The cryptographic module supports the following non-Approved function:

Table 3 – Non-Approved Algorithms

| Algorithm | Usage |
|---|---|
| PBKDF2 (non-compliant) | No claims are made to the security of non-compliant PBKDF2. Any keys derived from this function and used for protecting other keys are considered the equivalent to obfuscation or plaintext. |

If the service associated with the non-Approved PBKDF2 is invoked, it is implicitly assumed the module will transition to a non-Approved mode of operation.

## 2.2 Cryptographic Module Ports and Interfaces

The CryptoMod provides two Ethernet and two serial interfaces. The only interface available to users is the Web Config which is accessed through the Ethernet ports. The Serial Connector (COM 1) is used only for device to device connections.

The following table indicates the mapping of the module's physical ports and logical interfaces to the FIPS 140-2 interfaces.

Table 4 - Module Interface Mapping

| FIPS Interface | Physical Interface |
|---|---|
| **Data Input** | Ethernet interfaces (LAN 1, LAN 2), Serial connector (COM 1), Digital I/O |
| **Data Output** | Ethernet interfaces (LAN 1, LAN 2), Serial connector (COM 1), Digital I/O |
| **Control Input** | Ethernet interfaces (LAN 1, LAN 2), Reset Button, Switch 1 and 2 |
| **Status Output** | Ethernet interfaces (LAN 1, LAN 2), Front LED Panel (Figure 3), Ethernet port lights |

Figures 3, 4 and 5 as well as Tables 5, 6 and 7, show the mapping of the physical interfaces of the CryptoMod and their descriptions.

Figure 3 - Front Panel LED

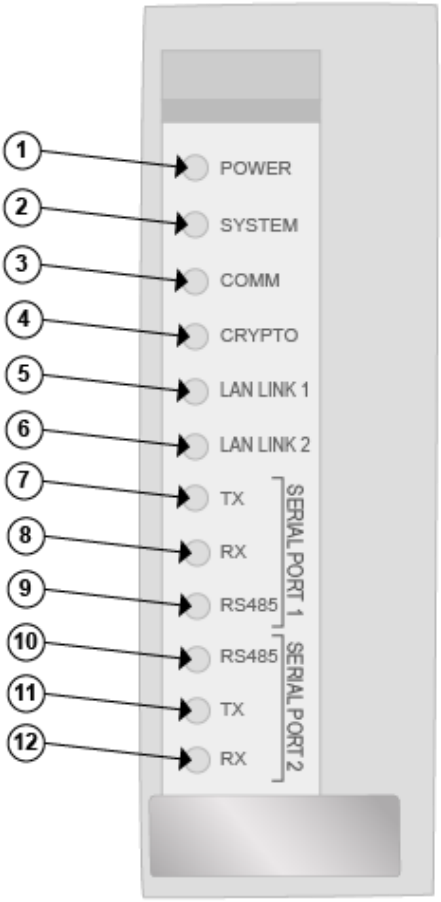


Table 5 - Front Panel LED Description

| Item | LED Name | Color | State | Description | |
|---|---|---|---|---|---|
| **1** | POWER | Green | On | The system is powered and booting the operating system. | |
| | | Red | On | 1. Initial power on state | |
| | | | | 2. Filesystem corrupted, OR Modified | |
| | | | | 3. Restore Client Settings - If Reset Button is pressed and held one second then released after LED changes to On solid. | |
| | | Red | Flashing | Reset Button is pressed. | |
| **2** | SYSTEM | Green | On | The system is powered and booting the operating system. | |
| | | Red | On | 1. Initial power on state | |
| | | | | 2. FILESYSTEM CORRUPT, MODIFIED, OR HACKED | |
| | | | | 3. Mounted peer on 5 (failover partition) | |
| **3** | COMM | Green | On | The system is powered and booting the operating system. | |
| | | Red | On | 1. Initial power on state | |
| | | | | 2. FILESYSTEM CORRUPT, MODIFIED, OR HACKED | |
| **4** | CRYPTO | Green | On | Secured Mode | |
| | | Red | On | 1. Initial power on state | |
| | | | | 2. Failed Startup Test | |
| | | None | Off | Unsecured Mode - Cryptographic Keys Zeroed | |
| **5** | LAN LINK 1 | Green | On | Active Ethernet Link | |
| **6** | LAN LINK 2 | Green | On | Active Ethernet Link | |
| **7** | TX | Red | On | Active Transmit Serial Data | Serial Port 1 (COM 1) |
| **8** | RX | Red | On | Active Receive Serial Data | |
| **9** | RS485 | Green | On | RS485 Mode | |
| | | Green | Off | RS232 Mode | |
| **10** | RS485 | Green | On | RS485 Mode | Serial Port 2 (COM 2-Disabled) |
| | | Green | Off | RS232 Mode | |
| **11** | TX | Red | On | Active Transmit Serial Data | |
| **12** | RX | Red | On | Active Receive Serial Data | |

Figure 4 – Top Side

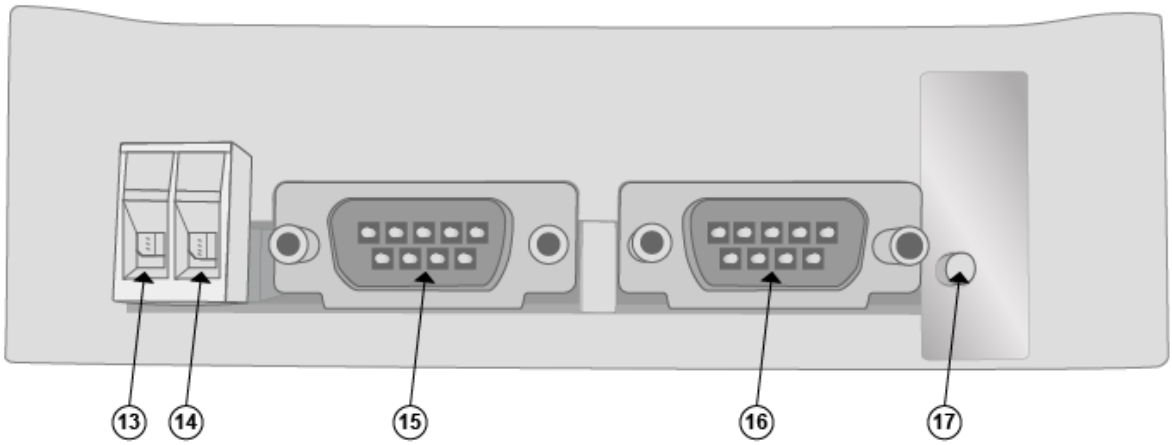



Table 6 - Top Side

| Item | Name | Description |
|---|---|---|
| **13** | Power Plug | +10 -26 VDC |
| **14** | | • GND 220mA |
| **15** | COM 2 | Serial Communication Port 2 (disabled) |
| **16** | COM 1 | Serial Communication Port 1 |
| **17** | RESET BUTTON | Restore Client Settings |

Figure 5 – Bottom Side

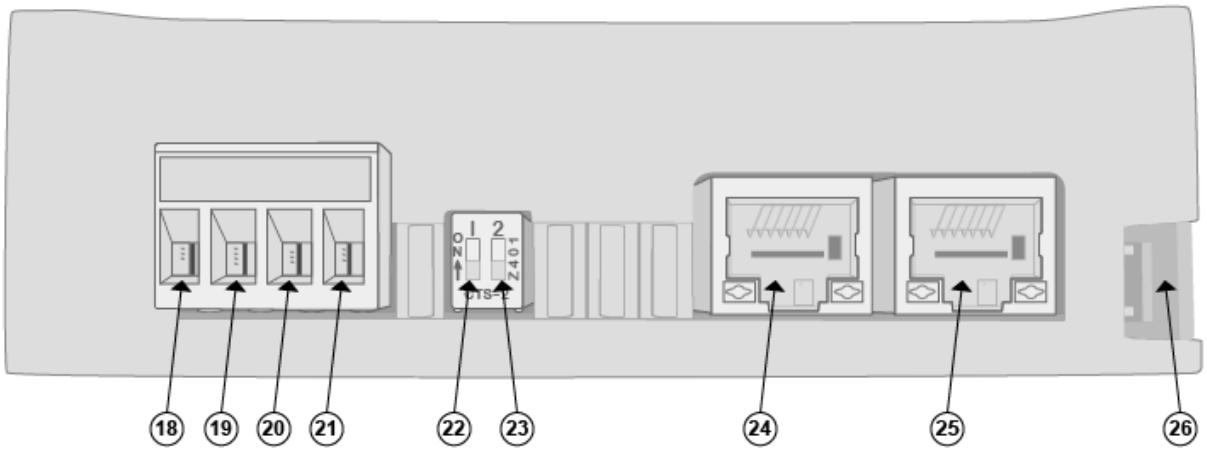



Table 7 - Bottom Side

| Item | Name | Number | State | Description |
|---|---|---|---|---|
| **18** | D I/O | 1 | 1 or 0 | Digital I/O #1 - type: Dry Contact, 1mA source, 3.3Vdc |
| **19** | | 2 | 1 or 0 | Digital I/O #1 - type: Dry Contact, 1mA source, 3.3Vdc |
| **20** | | 3 | 1 or 0 | Digital I/O #1 - type: Dry Contact, 1mA source, 3.3Vdc |
| **21** | | 4 | 0 | Earth Ground Connection Point |
| **22** | SWITCH | 1 | On | Disable Hardware Watchdog |
| | | | Off | Enable Hardware Watchdog - Default |
| **23** | | 2 | On | Enable On-board Lithium battery - Default (Required for FIPS) |
| | | | Off | Disable On-board Lithium battery |
| **24** | LAN 1 | LED Yellow | On | Ethernet Speed 100Mb |
| | | | Off | Ethernet Speed 10Mb |
| | | LED Green | On | Active Ethernet Link |
| **25** | LAN 2 | LED Yellow | On | Ethernet Speed 100Mb |
| | | | Off | Ethernet Speed 10Mb |
| | | LED Green | On | Active Ethernet Link |
| **26** | DIN RAIL MOUNT | | | DIN Rail Mount, Spring Loaded Locking Tab |

## 2.3 Roles, Services, and Authentication

The following sections provide details about roles supported by the module, how these roles are authenticated and the services the roles are authorized to access.

### 2.3.1 Authorized Roles

The CryptoMod supports role-based authentication. There are two security roles in the CryptoMod that operators may use: Crypto Officer and Crypto User.

- Crypto Officer (CO) - The Crypto Officer role performs administrative services on the module, such as initialization, configuration, and monitoring of the module. The module offers the Web Config as a management interface.
- Crypto User (CU) - The Crypto User role has the ability to perform basic configuration and monitoring operations using the Web Config provided by the CryptoMod.

The CryptoMod supports concurrent operators. Each user session requires an RSA certificate which is used to authenticate.

### 2.3.2 Authentication Mechanisms

The CryptoMod requires certificate based authentication for all users connecting via TLS or VPN. A username and password is also required for users to authenticate to the device via the Web Config.

Table 8 describes the authentication methods used.

**Table 8 - Authentication Mechanism Details**

| Role | Type Of Authentication | Authentication Strength |
|---|---|---|
| **Crypto Officer and Crypto User** | Username and Password | Passwords are a minimum of 8 characters, including at least one uppercase, one lowercase, one special character and at least one number. The password requirements are enforced by the Security Policy as well as Software.<br>The probability of a random correct password guess is less than $1/94^8$ (one (1) in 6,095,689,385,410,816). After a failed authentication attempt, the CryptoMod would allow another attempt within a second, thus the possibility of a random correct guess during a one-minute period is less than 60 * (1/6,095,689,385,410,816) which is less than 1/1,000,000 required by FIPS 140-2.<br>In order to successfully guess the sequence in one minute would require the ability to make over 101,594,823,040,180 guesses per second, which far exceeds the operational capabilities of the module. |
| | Certificate based authentication | CryptoMod supports public key authentication by using 2048 bit RSA keys. A 2048-bit RSA key has 112 bits, so the associated probability of a successful random attempt is 1 in $2^{112}$, which is less than 1 in 1,000,000 as required by FIPS 140-2. Assuming the module can support 60 authentications attempts in one minute, the probability of a success with multiple consecutive attempts in one-minute period is $60/2^{112}$ which is less than 1/100,000 |

### 2.3.3 Services

The CryptoMod provides a wide range of services and functions that allow the users to monitor and provide security for SCADA end devices. The table below displays the services provided by the CryptoMod and the access level required to perform them. All services are accessible through the Web Config.

The access types are abbreviated as follows
R = Read: The module reads the CSP(s).
W = Write: The module writes the CSP(s). This write access is performed after a CSP is either imported into the module, generated by the module, or if the module overwrites an existing CSP.
Z = Zeroize. The module zeroizes the CSP(s).

**Table 9 - Services**

| Service | Description | Role | | Key/CSP and Type of Access (Mapped from Table 10) | Access |
|---|---|---|---|---|---|
| | | CO | CU | | |
| **Change CO Password** | Apply a different password to the Crypto Officer | • | | 1,2,3,11,12,13,14,15,16, 17,18,19 | RW |
| **Change CU Password** | Apply a different password to the Crypto User | • | • | 1,2,3,11,12,13,14,15,16, 17,18,19 | RW |
| **Change Date and Time** | Apply a new date and time based on the current user's client side date and time. | • | | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **View/Modify Network Settings** | Apply different settings to IP addresses for Ethernet ports, gateways, DNS and subnets. | • | • | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **View/Modify Serial Port Settings** | Enable and disable serial port as well as the different configuration settings for it. | • | • | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **View/Modify SSL Tunnels Settings** | Create a new stunnel with a source and destination IP address, as well as source and destination port. | • | • | 1,2,3,11,12,13,14,15,16, 17 | RW |

| | | | | | |
|---|---|---|---|---|---|
| **View/Modify VPN Servers Settings** | Apply different settings to the listening port, protocol, routed networks/IP's, routed subnets as well as compression levels. | • | • | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **Create and Install Backups*** | Generation and Installation of a backup created from the CryptoMod's current settings. | • | | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17,18,19 | RW |
| **Create and Install PKI** | Generation and Installation of CA, Server and Client keyset, as well as a certificate revocation list. | • | | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17,18,19 | RWZ |
| **Enable/Disable Services** | Enable and disable services (Failover and ModBus). | • | | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **View and Export Log files** | Access log files from the CryptoMod. Download and view most recent log files as well as stored log archives. | • | • | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **Access the CryptoMod through OpenVPN** | Obtain access to the Web Config through OpenVPN on a configuration computer and the VPN running on the CryptoMod | • | • | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17 | RWZ |
| **Access the CryptoMod through Stunnel** | Obtain access to the Web Config through Stunnel on a configuration computer and Stunnel running on the CryptoMod | • | • | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17 | RWZ |
| **Apply Update** | Apply an update through the Web Config on the Package Manager page. | • | | 1,2,3,10,11,12,13,14,15, 16,17 | RW |
| **Import/Export Backup** | Import/Export backup created within the CryptoMod or imported from other CryptoMods. | • | | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17,18,19, 20,21 | RW |

| | | | | | |
|---|---|---|---|---|---|
| **Deleting Backup** | Deleting backup stored on the CryptoMod | • | | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17 | RWZ |
| **Restoring Backup** | Restoring latest imported/created Backup stored on the CryptoMod | • | | 1,2,3,4,5,6,7,8,9,11,12, 13,14,15,16,17 | RW |
| **On-Demand Self-Tests** | Reboot the module in order to perform self-tests | • | • | N/A | |
| **Display Status Information** | View module status through the Web Config. | • | • | 1,2,3,11,12,13,14,15,16, 17 | RW |
| **Zeroization** | Invoke the zeroization command in order to zeroize persistent keys stored in the CryptoMod | • | | 1,2,3,11,12,13,14,15,16, 17 | RWZ |

* This service utilizes a non-Approved PBKDF2. As stated in Section 2.1.2 of this document, a non-Approved mode of operation is implicitly assumed if this service is invoked. Keys derived and used by this non-Approved service are not associated or used by any other functions.

## 2.4 Physical Security

The CryptoMod's chassis is opaque within the visible spectrum. The enclosure of the module has been designed to satisfy Level 2 physical security requirements. Figures 6, 7, and 8 show the FIPS 140-2 level-2 tamper evident labels A and B (AUTOSOL P/N 729) applied to a CryptoMod. The two tamper evident labels are applied to the CryptoMod at the factory prior shipping.

Figure 6 – Tamper Evident Labels (A and B)

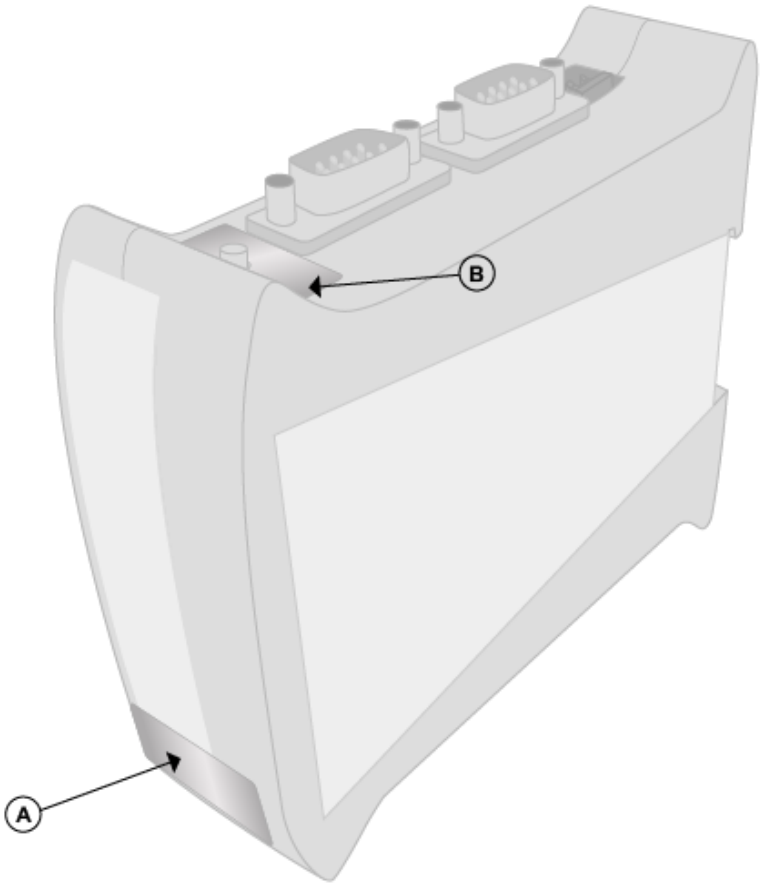
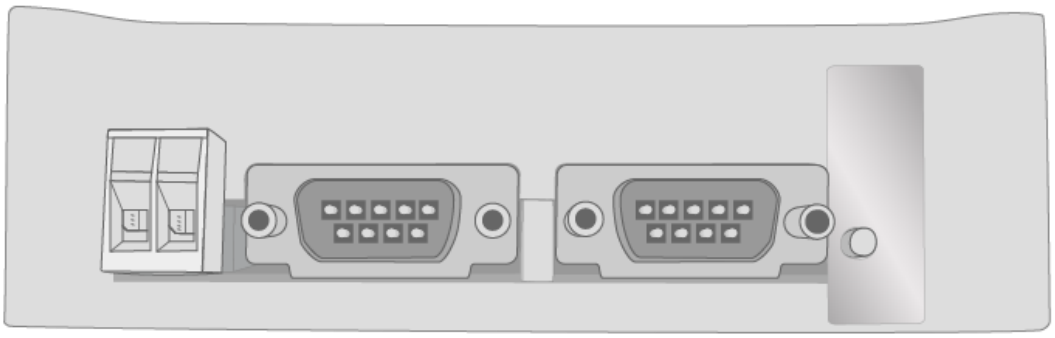


Figure 7 – Front -Tamper Evident Labels (A)


Figure 8 – Top -Tamper Evident Labels (B)



## 2.5 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the CryptoMod does not contain a modifiable operational environment.

## 2.6 Cryptographic Key Management

The CryptoMod uses public/private RSA keypairs for SSL and VPN operation as well as any HTTPS communication. The keypairs are shared between the applications that use them, there is not a separate keyset for each.

Table 10 - Details of Cryptographic Keys and CSPs

| ID | Key/CSP | Type | Generation/Input | Output | Storage | Zeroization | Usage |
|---|---|---|---|---|---|---|---|
| **1** | SSL/VPN Server Private Key | RSA 2048-bits | Generated on a CryptoMod, Installed through Web Config | Exported encrypted via Web Config | NVRAM plaintext | zeroize command | Used for SSL and VPN Server |
| **2** | SSL/VPN Server Public Key | RSA 2048-bits | Generated on a CryptoMod, Installed through Web Config | Exported encrypted via Web Config | NVRAM plaintext | zeroize command | Used for SSL and VPN Server |
| **3** | Certificate Authority Public Key | RSA 2048-bits | Generated on a CryptoMod, Installed through Web Config | Exported encrypted via Web Config | NVRAM plaintext | zeroize command | Used for SSL and VPN Server |
| **4** | Generated Server Private Key | RSA 2048-bits | Generated on a CryptoMod, Installed through Web Config | Exported encrypted via Web Config | NVRAM encrypted | zeroize command | Used for SSL and VPN Server |
| **5** | Generated Server Public Key | RSA 2048-bits | Generated Internally, or Input using Web Config | Exported encrypted via Web Config | NVRAM plaintext | zeroize command | Used for SSL and VPN Server |
| **6** | Generated Client Private Key | Private RSA 2048-bits | Generated Internally, or Input using Web Config | Exported encrypted via Web Config | NVRAM Encrypted | zeroize command | Used for SSL and VPN Server |

| ID | Key/CSP | Type | Generation/Input | Output | Storage | Zeroization | Usage |
|---|---|---|---|---|---|---|---|
| **7** | Generated Client Public Key | RSA 2048-bits | Generated Internally, or Input using Web Config | Exported encrypted via Web Config | NVRAM plaintext | zeroize command | Used for SSL and VPN Server |
| **8** | Generated CA Private Key | RSA 2048-bits | Generated Internally, or Input using Web Config | Exported encrypted via Web Config | NVRAM Encrypted | zeroize command | Used for SSL and VPN Server |
| **9** | Generated CA Public Key | RSA 2048-bits | Generated Internally, or Input using Web Config | Exported encrypted via Web Config | NVRAM Encrypted | zeroize command | Used for SSL and VPN ServeStored internally |
| **10** | Update Validation Public Key | RSA 2048-bits | Installed with build image unchangeable. | Does not exit the module | NVRAM plaintext | Fixed | Public Key for RSA SHA-256 validation of update packages |
| **11** | TLS Key Establishment Private Key | EC Diffie Hellman (256-bits), Diffie-Hellman (224-bit private exponent) | Generated internally | Does not exit the module | RAM plaintext | Reboot. Or automatically when TLS session is terminated | Used to negotiate TLS handshake and authentication |
| **12** | TLS Key Establishment Public Key | EC Diffie Hellman (256-bits), Diffie-Hellman (2048-bit public exponent) | Generated internally | Exits electronically in plaintext | RAM plaintext | Reboot. Or automatically when TLS session is terminated | Used to negotiate TLS handshake and authentication |

| ID | Key/CSP | Type | Generation/Input | Output | Storage | Zeroization | Usage |
|---|---|---|---|---|---|---|---|
| **13** | Web Config Passwords | Secret | CO/User provided | Does not exit the module | NVRAM plaintext | zeroize command | User Authentication |
| **14** | TLS pre-master secret | Shared Secret | Generated internally or enters electronically encrypted | Exits electronically encrypted | RAM plaintext | Reboot. Or automatically when TLS session is terminated | New TLS session keys can be created from this. |
| **15** | TLS master secret | 48-byte value | Generated internally | Does not exit the module | RAM plaintext | Reboot. Or automatically when TLS session is terminated | New TLS session keys can be created from this. |
| **16** | TLS session encryption key | AES (256-bits) | Generated internally | Does not exit the module | RAM plaintext | Reboot. Or automatically when TLS session is terminated | Key used to encrypt TLS session data |
| **17** | TLS session integrity key | HMAC (SHA1/256/384) | Generated internally | Does not exit the module | RAM plaintext | Reboot. Or automatically when TLS session is terminated | Used for TLS data integrity protection |
| **18** | V Value for NIST SP 800-90A Hash DRBG | Internal state value | Internally generated | Does not exit the module | RAM plaintext | Reboot, or upon DRBG uninstantpaiation | Internal value used by the Approved DRBG |

| ID | Key/CSP | Type | Generation/Input | Output | Storage | Zeroization | Usage |
|---|---|---|---|---|---|---|---|
| **19** | C Value for NIST SP 800-90A Hash DRBG | Internal state value | Internally generated | Does not exit the module | RAM plaintext | Reboot, or upon DRBG uninstantiation | Internal value used by the Approved DRBG |
| **20** | Data Protection Key | AES (256-bits) | Derived internally via PBKDF2 function | Does not exit the module | RAM plaintext | Reboot, Upon completion of PBKDF2 function | Key used for storage applications |
| **21** | Certificate Chain Protection Password | Secret | CO/User provided | Does not exit the module | N/A | Reboot, Upon completion of PBKDF2 function | Password input to PBKDF2 function |

### 2.6.1 Key Generation

Keys in the CryptoMod are generated using the Approved NIST SP 800-90A DRBG which is seeded by an internal entropy source. The minimum number of bytes of entropy generated directly by the CryptoMod for use in key generation is 32 bytes (256 bits).

The module performs PBKDF2 as defined in IETF25 RFC26 #2898. The vendor affirms compliance with SP 800-132, using option 1(a) in Section 5.4 to derive the Data Protection Key (DPK). The PBKDF2 is used for storage applications only.

- Passwords used in key derivation are minimum 8 characters, including at least one uppercase, one lowercase, one special character and at least one number. The password requirements are enforced by the Security Policy as well as Software.
- The probability of a random correct password guess is less than $1/94^8$ (one (1) in 6,095,689,385,410,816).
- In order to successfully guess the sequence in one minute would require the ability to make over 101,594,823,040,180 guesses per second, which far exceeds the operational capabilities of the module.

### 2.6.2 Key Entry/Output

To operate the CryptoMod a keyset will need to be installed by the Crypto Officer. In order to install the keyset, the Crypto Officer shall first authenticate to the Web Config and then navigate to the PKI page. The keyset consists of three files: Certificate Authority (Table 10 #8,#9), Server Certificate (Table 10 #4,#5) and Certificate Revocation List (CRL). The files can be downloaded from the CryptoMod that generated them.

The installation of keys into the CryptoMod requires entry of the Certificate Chain Protection Password (Table 10 #21) used when the keyset was originally created.

All keys, authentication and sessions in the CryptoMod are encrypted over TLS 1.2.

### 2.6.3 Zeroization Procedures

Key zeroization is achieved by overwriting the key storage partition with binary zeros. As described in Table 10 - Details of Cryptographic Keys and CSPs, zeroization for persistent keys takes place by triggering the zeroize command. The zeroize command can be found in the PKI page in the Web Config, under Install PKI. This function will also force a reboot of the CryptoMod, which would terminate any ongoing sessions.

In other cases, ephemeral keys are zeroized upon terminating the established session or a reboot of the device.

## 2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The module is declared to conform with EMI/EMC requirements for a Class B (business use) device as specified by Part 15, Subpart B, of the FCC rules.

## 2.8 Self-Tests

Self-tests are health checks performed automatically by CryptoMod which ensure that the cryptographic algorithms within the module are operating correctly.
The self-tests identified in FIPS 140-2 broadly fall within two categories

1. Power-On Self-Tests
2. Conditional Self-Tests

### 2.8.1 Power-On Self-Tests

All Power-On Self-Tests automatically run upon boot up of the CryptoMod. Upon success of the Power-On Self-Tests, the SYSTEM light in the front LED panel (Figure 3) will become green. An operator can initiate the power-up self-tests on demand by shutting down and restarting the CryptoMod with the Reboot CryptoMod function in the Web Config page under Administration > System Settings.

Table 11 shows the Power-On Self-Tests the CryptoMod runs on startup.

**Table 11 - Power-On Self-Tests**

| Algorithm | Type | Description |
|---|---|---|
| Firmware Integrity | Integrity test | SHA-256 integrity test performed at start-up on the operational firmware |
| Cryptographic Library Integrity Test | Integrity test | HMAC-SHA1 integrity test performed on the cryptographic library |
| AES | KAT | Encrypt/Decrypt CBC mode: 256 key length |
| RSA | KAT | Sign and verify using 2048 bit key and SHA-256 |
| DRBG | KAT | HASH_DRBG |
| HMAC | KAT | One KAT per SHA-1, SHA-256 and SHA-384 |
| SHA | KAT | SHA-1, SHA-256 and SHA-384 on known data. Resulting hash compared to a known good value |

### 2.8.2 Conditional Self-Tests

Table 12 - Conditional Self-Tests

| Algorithm | Test |
|---|---|
| DRBG | Health Checks required by Section 11 of NIST SP 800-90Arev1 |
| RSA | Pairwise consistency test on each generation of a key pair |
| CRNGT | Continuous RNG test run on outputs of DRBG and the NDRNG used to seed the Approved DRBG. The continuous test is performed every time a random seed is generated. It is tested against the previous generated seed to assure it is unique. |
| Firmware Load Test | Firmware load test using an RSA 2048-bit Signature Verification operation |

### 2.8.3 Self-Tests Error Handling

Upon failure of a self-test, the SYSTEM light in the front LED panel (Figure 3) will become red and the CryptoMod will attempt at fixing itself by rebooting. This could continue indefinitely if the attempts fail. The Web Config and any cryptographic operation will be inhibited until the self-tests successfully pass.

## 2.9 Mitigation Of Other Attacks

The CryptoMod does not claim to mitigate any attacks in a FIPS-approved mode of operation.

# 3. Secure Operation

When in FIPS-approved mode the CryptoMod has only one image installed at any given time and utilizes only supported algorithms (Table 2 in section Modes of Operation) to operate.

## 3.1 Setup and Initialization

In order to operate in a FIPS-approved mode of operation the Crypto Officer (CO) must initialize and operate the CryptoMod using the steps below.

1. Boot the CryptoMod.
   - For better security, it is recommended that the CryptoMod's Ethernet Interface (LAN 1 or LAN 2 port be connected directly to the Crypto Officer's configuration computer's ethernet port).
   - For more information, visit the "*Establishing a Connection to the CryptoMod"* section of the User Manual shipped with the CryptoMod.
2. As the CO, access the CryptoMod's Web Config page through https:// IP of the CryptoMod
   - If connected to LAN 2 port of the CryptoMod go to: https://172.16.63.3
   - Default IP of the CryptoMod's LAN 1 port is 172.16.63.2
3. The CO shall change the default CO and CU passwords via the Web Config.
   - Visit the Passwords page under the Administration menu.
   - After each password change the Web Config will terminate the session and force the CO to reauthenticate using the new password.
   - Reauthentication will occur three times: after changing the default CO password, after changing the default CU password, and reauthenticate the third time to continue with these steps.
4. As the CO, create a Keyset (consisting of the Generated Certificate Authority (CA) Key Pair (Table 10 #8,9), Generated Server Key Pair (Table 10 #4,#5) and Certificate Revocation List file) via the Web Config.
   - Select create PKI in the PKI page under the Administration menu.
   - For more information, please consult *Creating a PKI* in the User Manual.
5. The CO must then export the created Keyset to the CO's configuration computer using the PKI page.
   - The keyset will be available for download in the PKI page after creation in step 4.
   - Export the CA (ca.crt) and CRL(currentlist.crl.pem)
   - Export the Server Certificate (file name contains 'SVR')
   - Export the Client Certificates (file name ends in BROWSER.key.crt.pfx and other file ends in stunnel.ovpn.crt)
6. The CO shall now install the downloaded Keyset via the Web Config.
   - Select Install PKI in the PKI page under the Administration menu.
   - Upload the CA file(ca.crt), the Server Certificate file (file name contains 'SVR'), and the CRL file(currentlist.crl.pem).

- For more information, please consult *How to use a PKI* in the User Manual.

7. Click *Start Change PKI Process* in the PKI page.
8. Click *Reboot CryptoMod* in the PKI page.
9. While the reboot is taking place, install the client certificate (Table 10 #6,#7 file name ends in BROWSER.key.crt.pfx) and the CA (ca.crt) that were downloaded in step 6 in the browser of the configuration comptuer.
    - For more information, please consult *Installing certificates in browser* in the User Manual.
10. Enter the Web Config of the CryptoMod after installing the browser certificates and ensure it displays “Mode of Operation: FIPS-Approved” mode in the side Unit Statistics table.
11. Ensure the crypto LED goes green on the Front Panel of the CryptoMod.
    - Figure 3 specifies the LED, which when green indicates the module is in the approved mode of operation.
    - After the approved mode of operation is verified, the CO can generate a keyset for the CU.

# Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Table 13 - Acronyms

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| CA | Certificate Authority |
| CRL | Certificate Revocation List |
| CMVP | Cryptographic Module Validation Program |
| CO | Crypto Officer |
| CU | Crypto User |
| CSP | Critical Security Parameter |
| DRBG | Deterministic random bit generator |
| FIPS | Federal Information Processing Standard |
| HTTP | Hyper Text Transfer Protocol |
| KAT | Known Answer Test |
| LED | Light Emitting Diode |
| MAC | Message Authentication Code |
| NIST | National Institute of Standards and Technology |
| NVRAM | Non-Volatile Random-Access Memory |
| PBKDF2 | Password-Based Key Derivation Function 2 |
| PKI | Public Key Infrastructure |
| RAM | Random Access Memory |
| RSA | Rivest Shamir and Adleman method for asymmetric encryption |
| SHA | Secure Hash Algorithm |
| SSL | Secure Sockets Layer |
| SVR | Server |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |