APCON Inc.

ACI-3002-S Controller

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.1

Date: 7/15/16

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the APCON ACI-3002-S controller module, hereafter denoted the Module. The Module is a Linux based control module designed to manage and control APCON's XR series product line. The Module is made of commercial grade components and meets FIPS 140-2 Level 2 requirements.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	ACI-3002-S Controller	ACI-3002-S, Version 1.0	5.07.1 build 106

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Cryptographic module. The Module is a multi-chip embedded embodiment; the cryptographic boundary is restricted to the module. (The module is utilized in the APCON XR chassis and performs the same function in each.)

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1: The module with the conformal coating protects the physical cryptographic boundary from intrusion. Any attempt to tamper with the module will result in physical evidence in the coating. The six components protruding from the conformal coating are DC/DC power regulators which are not security relevant. There are visible two heatsinks which are also not security relevant have been excluded from the requirements of FIPS 140-2.

Figure 1 depicts the module's internal and external ports as well as the physical pieces of the hardware.

Figure 1 – Module- ACI-3002-S Controller

The Module relies on a serial connection, HTTP and HTTPS using the LAN ports to connect to the network. There is no debug output on the controller.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
LAN 1 (RJ-45)	Port is used to access the controller via: HTTP and HTTPS	Data in | Data out | Status out | Control in
LAN 2 (RJ-45)	Port is used to access the controller via: HTTP and HTTPS	Data in | Data out | Status out | Control in
USB port	Disabled/Inactive	
SD card slot	Disabled/Inactive	
Serial	Port is used to connect the serial port to the COM port on a host laptop or desktop. Enable the serial console log-in (which is password-protected), and configure the chassis using CLI commands.	Data in | Status out | Control in
Backplane connecter	This connecter is located at the rear of the control card and connects into the backplane of the chassis.	Data in | Data out| Status out | Control in
Power connection	Located next to the backplane connecter this port supplies power to the Control card from the chassis.	Power in
LEDs	The status LED is green when the module is powered on. There are various combinations showing error states. (In User Guide pg. 12)	Status out

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and cryptographic boundary.

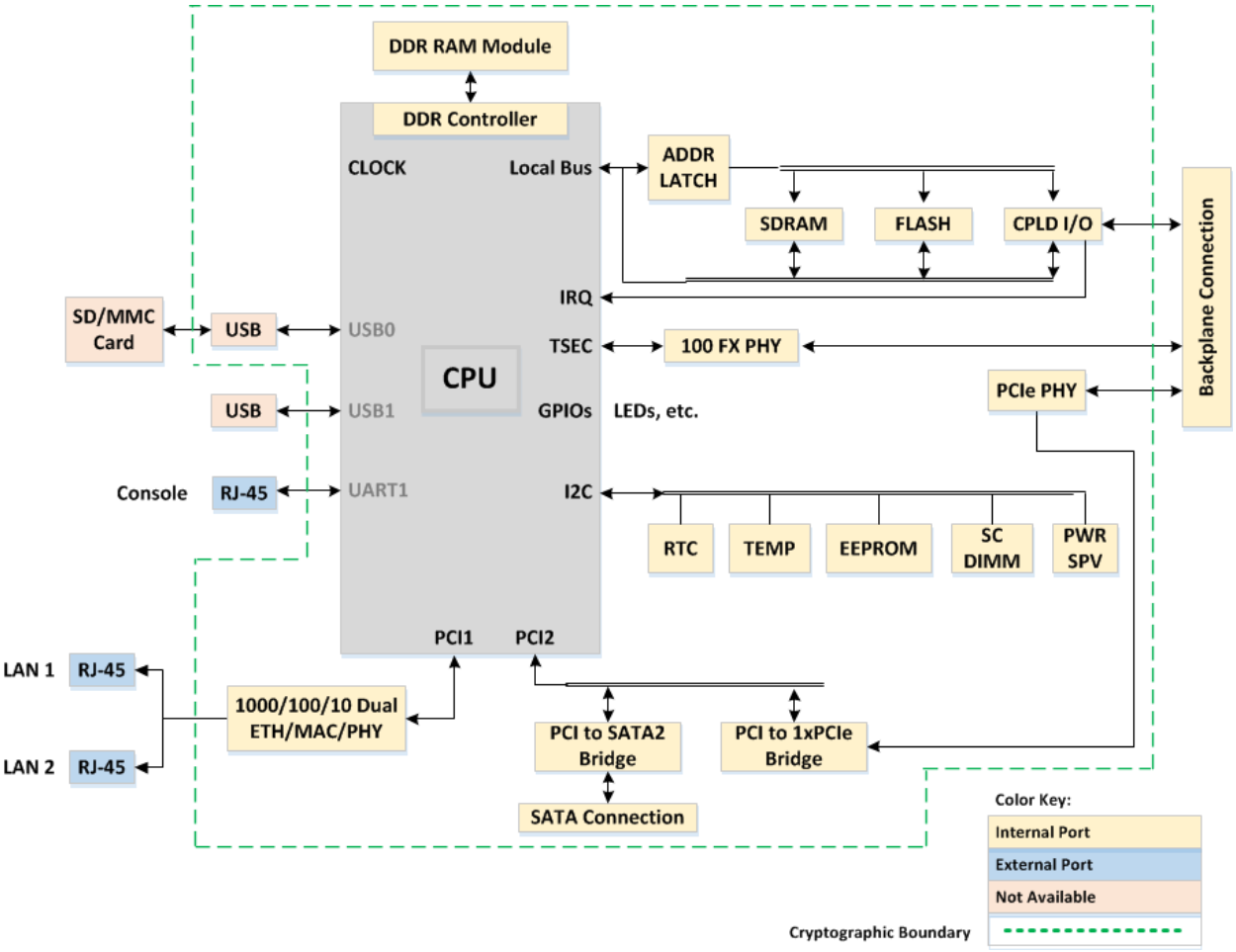

Figure 2 – Module Block Diagram

1.3 Approved Mode of Operation

The module is in the Approved mode of operation as long as the user does not load an RSA-4096 key pair for the RSA KDK/SGK (see CSP table). To verify that a module is functioning correctly in the Approved mode of operation, access the WebX GUI and verify that 1) the "FIPS 140-2 Mode" indicator is present, and 2) the GUI is not provided over an HTTPS connection secured with an RSA-4096 certificate. Please see User Guide Section 4 for initialization steps and follow all recommendations.

1.4 Cryptographic Functionality

The Module implements the FIPS 140-2 Approved as well as Non-Approved but Allowed cryptographic functions listed in the tables below. Note that some certificates cover algorithm variants which are not supported by the module (e.g., SHA Cert #3186 covers SHA-512, which is not used).

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Key sizes: 128, 256 bits Block Cipher modes: CBC	3866
AES-GCM	[SP 800-38D] Functions: Authenticated Encryption, Authenticated Decryption Key sizes: 128, 256 bits	3866
AES Key Wrap	[SP 800-38F §3.1] Functions: Key Wrap, Key Unwrap Variant 1: AES-128-CBC or AES-256-CBC, and HMAC Variant 2: AES-128-GCM or AES-256-GCM	3866
DRBG	[CTR-DRBG [SP800-90A]] Functions: CTR DRBG Security Strength: 256 bits	1100
HMAC	[FIPS 198] Functions: Message Digests SHA Sizes: SHA-256, SHA-384	2510
RSA	[FIPS 186-4] Function: Signature Generation (PKCS #1 v1.5) Key sizes: 2048, 3072 bits SHA sizes: SHA-256, SHA-384 Function: Signature Verification (ANSI X9.31) Key sizes: 2048 bits SHA sizes: SHA-256	1974

Algorithm	Description	Cert #
SHA	[FIPS 180-4] Function: Signature Generation SHA sizes: SHA-256, SHA-384 Function: Signature Verification SHA sizes: SHA-256 Function: HMAC SHA sizes: SHA-256, SHA-384 Function: Password Hash (Single Iteration) SHA sizes: SHA-256	3186
CVL (TLS v1.2 KDF)	[SP800-135] SHA sizes: SHA-256, SHA-384	743

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
RSA Key Transport	Functions: Asymmetric Decryption Key sizes: 2048,3072 bits
ECDH	Functions: Key Exchange Curves/Key sizes: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571

Table 6 – Protocols Allowed in FIPS Mode

Protocol	Description
TLS v1.2	[IG D.8 and SP 800-135] Cipher Suites: ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 AES256-GCM-SHA384 AES256-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 AES128-GCM-SHA256 AES128-SHA256

The TLS protocol has not been tested by the CAVP and CMVP.

Non-Approved Cryptographic Functions for use in non-FIPS 140-2 mode only:

- RSA-4096 Signature Generation
- RSA-4096 Asymmetric Decryption

1.5 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4. The CSP names are generic, corresponding to API parameter data structures.

Table 7 – Critical Security Parameters (CSPs)

CSP	Description / Usage
RSA KDK/SGK	RSA (2048, 3072) private key, used for key decryption (private key transport) or signature generation, depending on the TLS cipher suite in use.
ECDH Private	ECDH (All NIST defined and SP800-131A-compliant B, K, and P curves) private key agreement key.
AES EDK	AES (128, 256) encrypt / decrypt key. Can be used for Key Wrap and Key Unwrap.
DRBG Internal State	"V" and "Key" values for the SP800-90A CTR DRBG. Seeded by "Entropy String"
HMAC Key	Keyed hash key SHA-256, SHA-384. Can be used for Key Wrap and Key Unwrap.
TLS pre_ master_secret	The pre_master_secret value for TLS. Derived via RSA key transport or ECDH exchange; used to create the AES EDK and HMAC Key via the TLS KDF.
Admin passwords	Strings used for admin login, one per authorized identity. Only the SHA-256 hash is stored in NVM.
Advanced Operator passwords	String used for advanced operator login, one per authorized identity. Only the SHA-256 hash is stored in NVM.
Basic Operator / Guest passwords	String used for basic operator (guest) login, one per authorized identity. Only the SHA-256 hash is stored in NVM.
Entropy String	Unique 1024 byte random bytes loaded at factory from desktop workstations with their own entropy sources (spinning disk drives, mouse and keyboard interrupts). It is used to seed the OpenSSL DRBG with enough entropy to saturate its state. It is replaced with a new seed immediately upon usage.

1.6 Public Keys

Table 8 – Public Keys

Key	Description / Usage
RSA SVK	RSA (2048) signature verification public key for firmware load.
RSA KEK/SVK	RSA (2048, 3072) public key. This is provided to the client during a TLS handshake, and not used by the module directly. The client uses it for key encryption (public key transport) or signature verification, depending on the TLS cipher suite in use.
ECDH Public	EC DH (All NIST defined and SP800-131A compliant B, K and P curves) public key agreement key for TLS handshakes.

2 Roles, Authentication and Services

2.1 Assumption of Roles

The module supports three distinct human operator roles, Admin, Advanced Operator and Basic Operator/Guest. The cryptographic module enforces the separation of roles using an internal role-based privilege schema. The module also supports a fourth role, Firmware Update, for the exclusive purpose of machine-to-machine authenticated firmware distribution with a chassis. Re-authentication is enforced after module reset and when changing roles.

The module uses a username and password to authenticate the human roles and a digital signature to authenticate the Firmware Update role. Both methods use identity-based authentication.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Admin	Admin has full privileges to the module including key loading and configuration.	Identity-Based	Username Password
Advanced Operator	Operational use of the module. (switch configuration)	Identity-Based	Username Password
Basic Operator / Guest	Read-only access (default settings).	Identity-Based	Username Password
Firmware Update	Intra-chassis firmware update	Identity-Based	RSA-2048 signature

2.2 Authentication Methods

2.2.1 Password Authorization

When you select an Internal (or local) database, you must also configure the password. To ensure greater security, APCON recommends the use of strong passwords when logging into the Module. When the module starts, the core daemon initializes its list of logged in users to empty. The logged in user file is erased and this process happens every time a power cycle occurs.

Password strength is restricted to “Medium” (Requires at least 8 characters) or Higher. The default password setting is “Medium”.

Rules enforced by “Strong” Password Recommendations:

- All keyboard characters are allowed and there is no restriction to using alphabetical or numeric characters or symbols for a password.
- Must contain a minimum of eight (8) alphanumeric characters.
- Must contain a maximum of 63 alphanumeric characters.
- At least one uppercase letter (alpha character).
- At least one lowercase letter (alpha character).
- At least one special character (a digit or symbol).

Password Rationale

APCON passwords allow ASCII characters 32 through 126 and require a minimum password length of 8 characters. Thus the password space is 95^8 ~= 6.634204312890625 * 10^15 (approximately 6.63 quadrillion) possible passwords. A single random guess would have a 1 in 6.63 quadrillion chance of being correct which is far less than 1 in 1,000,000.

The module allows for five login attempts before locking down. It then allows a single login attempt every ten minutes. For the initial five logins the probability of false authentication is 5 in 6.63 quadrillion, which is less than one in 100,000.

2.2.2 Intra-Chassis Firmware Loading Authentication

It is possible for one module to provide firmware to another via the chassis backplane. The firmware is authenticated separately by each module undergoing the upgrade, using an RSA-2048/SHA-256 signature check. (The verification key is RSA SVK; see the Public Keys table.) Aside from the entry point, this process is identical to human-initiated firmware loading. If authentication fails, the firmware is rejected.

Authentication Strength Rationale

The firmware signature provides the authentication necessary for the Firmware Update role. RSA-2048 has a security strength of 112 bits, so it can be said that a random attempt to crack the key will have a success probability of 2^-112, which is less than 1 in 1,000,000. If a well-resourced attacker can make one quadrillion attempts in one minute, the success probability will be slightly under 2^-60, which in turn is less than 1 in 100,000.

2.3 Services

All services implemented by the Module are listed in Table 12. Each service description also describes all usage of CSPs by the service.

Table 10 – Authenticated Services

Service	Description	Admin	Advanced Operator	Basic Operator/ Guest	Firmware Update
Reboot by command	Module power cycles and self-tests are performed (FIPS_selftest). Does not access CSPs.	X			
Zeroize by human operator	Zeroize command delivered by a human operator. Commands the secondary controller module in the chassis, if present, to also zeroize (see "Zeroize by intra-chassis"); overwrites all CSPs with zeroes.	X			
View Switch Settings	Users read only permissions to multiple configurations of the switch.	X	X	X	
Configure the switch	Users can configure blade functionality including new connections and aggregations.	X	X		
Configure the module	Users can configure all module features including network settings, SSL Certificates, Date/Time, ETC. for the module.	X			
Load new firmware	Load signed firmware into the module	X			X

Table 11 - Unauthenticated Services

Service	Description
FIPS-Mode Banner	This is shown on the login page, help-> about page, as well as in the CLI. It is green if the module is operating in FIPS mode and red if the module is in an error state.
Hard Reboot	Reboot caused by loss of power.
Zeroize by intra-chassis	When this module is functioning as the secondary module in the chassis, the primary module can send it a command to zeroize. Aside from the entry point, this behaves the same as "Zeroize by human operator".

The module uses a serial connection, HTTP and HTTPS services as management interfaces. They serve only to manage the blades and settings of the switch. All require login credentials to communicate; there are no interfaces that can connect to the module without authentication.

Table 12 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: Reads the CSP out to an external port. (i.e., it exports the CSP.)
- E = Execute: Use the CSP for a cryptographic operation.
- W = Write: Writes arbitrary data to the CSP. Excludes random generation and zeroization.
- Z = Zeroize: Write zeros or random garbage to the CSP.

Table 12 – CSP Access Rights within Services

Services	CSPs								
	RSA KDK/SGK	ECDH Private	AES EDK	DRBG State	HMAC Key	Admin passwords	Adv. Op passwords	Basic Operator Guest passwords	Random String
Reboot (either method)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Zeroize (either method)	Z	Z	Z	Z	Z	Z	Z	Z	Z
View Switch Settings	E	GEZ	GEZ	N/A	GEZ	N/A	N/A	N/A	N/A
Configure the switch	E	GEZ	GEZ	N/A	GEZ	N/A	N/A	N/A	N/A
Configure the Module	REW	GEZ	GEZ	N/A	GEZ	W	W	W	N/A
Load new firmware	E	GEZ	GEZ	N/A	GEZ	N/A	N/A	N/A	N/A
FIPS-Mode Banner	E	GEZ	GEZ	N/A	GEZ	N/A	N/A	N/A	N/A

3 Self-tests

Each time the Module is powered up, it tests that the cryptographic algorithms are still operating correctly. Power up self–tests are available on demand by power cycling.

On power up or reset, the Module performs the self-tests described in Table 13 below. All self-tests must be completed successfully prior to any other use of cryptography by the Module. If one of the tests fails, the Module enters an error state. This can only be cleared by performing a hard reboot. During boot or anytime a KAT is run manually there is no debug output available.

If the Firmware Integrity test fails, the module enters the Soft Error State 2. For any of the other power-on self-test failures, it enters the Soft Error State. Either error state can be cleared with a power cycle.

Table 13 – Power Up Self-tests

Test Target	Type	Description
HMAC	KAT	One KAT per SHA-256 and SHA-384. Per IG 9.3, this testing covers SHA POST requirements.
AES	KAT	Separate encrypt and decrypt, ECB mode, 128 bit key length.
RSA	KAT	Sign and verify using 2048 bit key, SHA-256, PKCS#1 v1.5.
DRBG	KAT	CTR_DRBG: AES, 256 bit with derivation function Performs Instantiate and Generate health tests as per SP800-90A
ECDH	KAT	Key-gen, sign, verify using P-224.
Firmware integrity	CRC	CRC 16 on the Firmware binary

Table 14 – Conditional Self-tests

Test Target	Description
Firmware Load	RSA 2048 bit signature verification performed when firmware is installed. Algorithm: RSA w/ SHA-256
SP 800-56A Assurances	Using a non-compliant-SP800-56A-implementation for ECDH. Using the OpenSSL (compiled with OpenSSL FIPS Object module) FIPS 140-2 continuous self-test pairwise consistency test for ECDH.
Continuous RNG	Continuous RNG test per FIPS 140-2 4.9.2. Performed on DRBG.
SP800-90A DRBG health tests	Performs the Reseed DRBG health test as per SP800-90A.

4 Physical Security Policy

The physical security for the controller board is provided by coating the controller board with an opaque Conformal coating. The coating is black in color, covers the relevant components and will display signs of tampering. See Table 16 for further information.

Table 15 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
All encryption components are contained on the controller board. The controller board will have a tamper-evident Conformal coating. The Conformal coating is an epoxy, deep blue/black in color that covers all security related components.	Once every six months.	The controller boards must be removed from the chassis for inspection of the components and Conformal coating. To check, remove and examine the controller board to determine if the controller has been tampered with by looking for: • Areas where the coating has been scraped off or removed with a solvent. • Discolored patches that don't match the rest of the coating. This indicates that the original coating may have been removed and then touched up. • Holes in the coating in areas such as component legs. This indicates that a probe was used to access a component.

5 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

6 Mitigation of Other Attacks Policy

The module is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

7 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The module provides four distinct operator roles: Admin, Advanced Operator, Basic Operator / Guest, and Firmware Update.
2. The module provides role-based authentication for Firmware Update, and identity-based authentication for the other roles.
3. The module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The operator is be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module uses an SP800-90A DRBG and thus does not make use of the seed/seed-key architecture.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module supports concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support manual key entry.
14. The module does not have any external input/output devices used for entry/output of data.
15. The module does enter plaintext CSPs but does not output them.
16. The module does not output intermediate key values.

8 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[FIPS186-4]	*The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)*, May 2014
[SP800-56A]	*Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013
[SP800-90A]	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012

Table 17 – Acronyms and Definitions

Acronym	Definition
KDK	Key Decryption Key
SGK	Signature Generation Key
EDK	Encryption / Decryption Key
NVM	Non-Volatile Memory
SVK	Signature Verification Key
KEK	Key Encryption Key
CLI	Command Line Interface
ACI-3002-S Controller	The module
APCON XR chassis	Parent device in which this module is embedded.