2055 Gateway Place
Suite 650
San Jose, CA 95110

T 408.841.4700
info@vcinity.io
Vcinity.io

(33-0206-013 Rev C)

Vcinity, Inc.

RAD X-1040 AES-256

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

(33-0206-013 Rev D)

Document Revision: 1.0
H.W. Version: RAD X-1040 (90-0206-101) Rev L
S.W. Version: NA
F.W. Version: RAD X Release 4.0.1

This is a FIPS 140-2 non-proprietary Security Policy; may be reproduced only in its original entirety without changes or revision.

REVISION HISTORY

Author(s)	Version	Updates
Vcinity team	**33-0206-013 Rev D**	**Initial Release**

Table of Contents

INTRODUCTION 3
CRYPTOGRAPHIC BOUNDARY 4
FIPS 140-2 MODES OF OPERATION.......... 5
ACRONYMS 5
SECURITY LEVEL SPECIFICATION 6
PHYSICAL PORTS AND LOGICAL INTERFACES 6
SECURITY RULES 7
CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS 9
IDENTIFICATION AND AUTHENTICATION POLICY 10
CRYPTOGRAPHIC MODULE SERVICES and ACCESS CONTROL 11
ALGORITHMS 14
APPROVED ALGORITHMS 14
NON-APPROVED ALGORITHMS USED IN FIPS APROVED MODE 15
NON-APPROVED ALGORITHMS USED IN THE NON-FIPS MODE OF OPERATION 15
SELF-TESTS 16
OPERATIONAL ENVIRONMENT 17
PHYSICAL SECURITY POLICY 17
MITIGATION OF OTHER ATTACKS POLICY 17

INTRODUCTION

The Vcinity, Inc. RAD X-1040 AES-256 Cryptographic Module (H.W. Version: RAD X-1040 (90-0206-101) Rev L; S.W. Version: NA; F.W. Version: RAD X Release 4.0.1) is a multi-chip standalone cryptographic module designed to provide low latency, high performance, secure connectivity on a global scale. Allowing businesses to take command of geographically dispersed compute and storage resources, with the immediacy of local access.

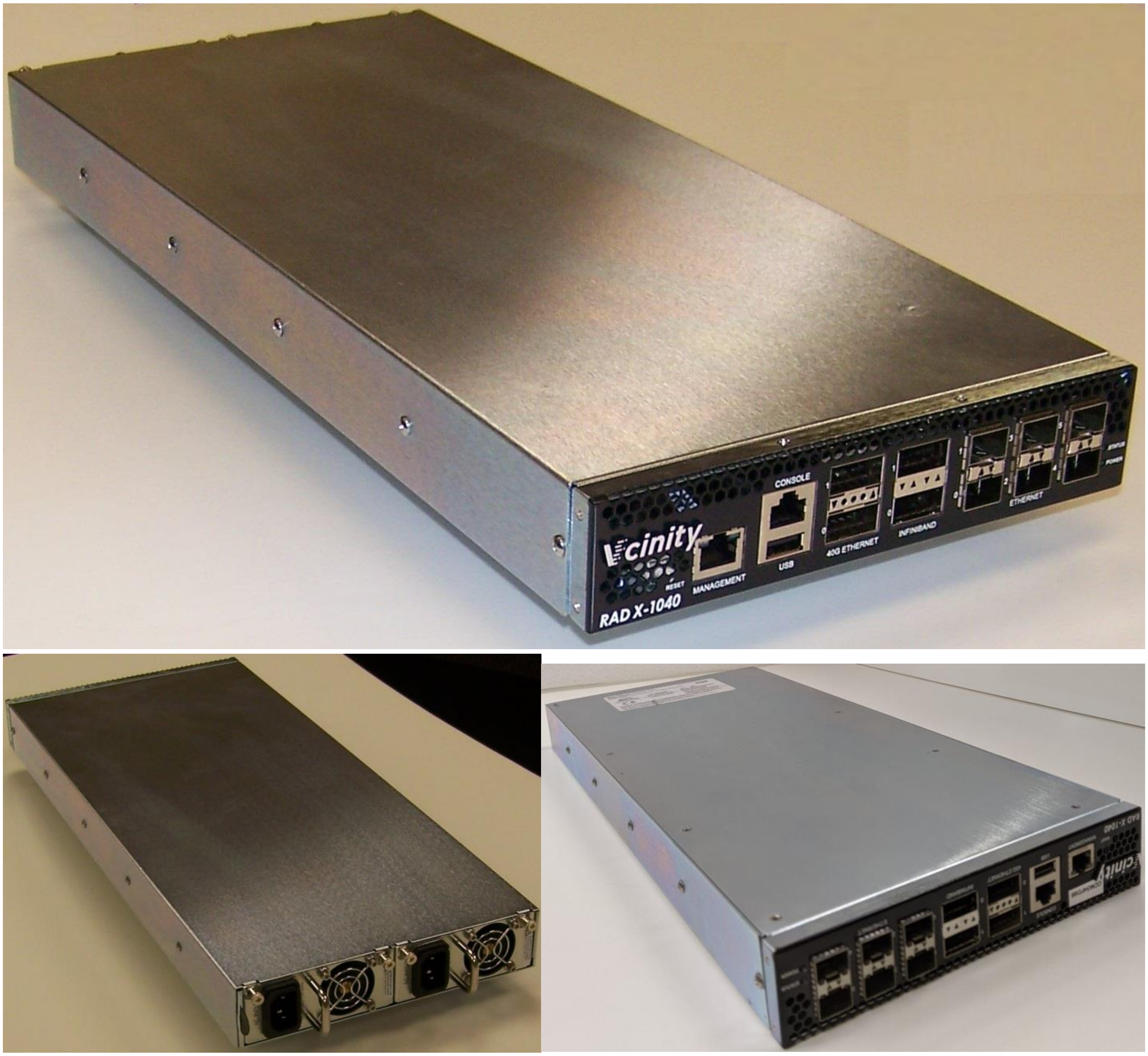

Exhibit 1 – *Representative Photos of the RAD X-1040 AES-256 Cryptographic Module*

CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary is defined as the outer perimeter of the RAD X-1040 enclosure. The enclosure is fabricated from mild steel, 20 Gauge, 0.0359in. thick. The following block diagram illustrates the cryptographic boundary:

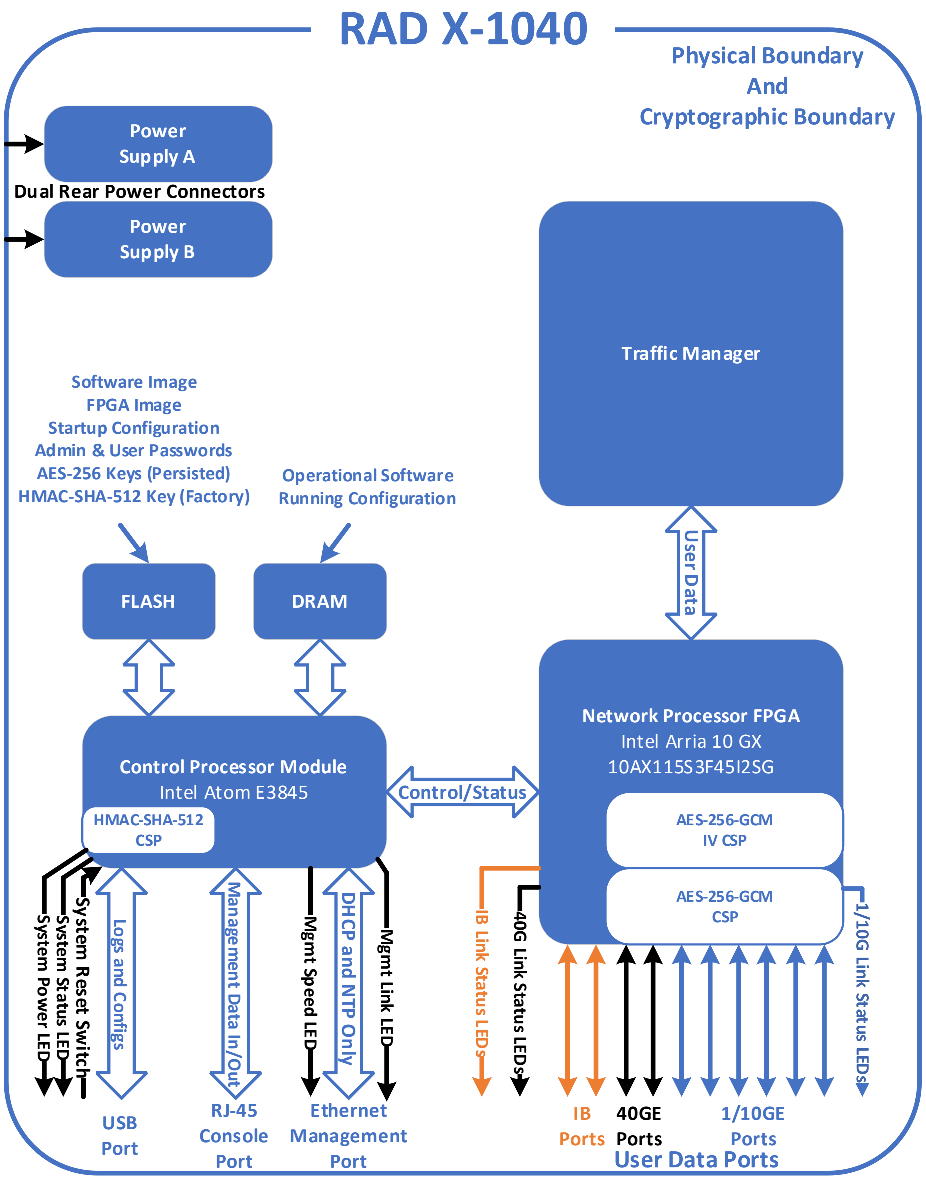

Exhibit 2 – *Specification of Cryptographic Boundary*

The Control Processor Module (Intel Atom E3845) uses the HMAC-SHA-512 algorithm to validate firmware downloads to the system. The HMAC-SHA-512 algorithm calls the SHA-512 algorithm. The Network Processor FPGA (Intel Arria 10 GX, 10AX115S3F45I2SG) uses the AES-GCM algorithm to encrypt and authenticate the data in flight.

FIPS 140-2 MODES OF OPERATION

This module supports both an Approved mode of operation and a Non-Approved mode of operation. In the Approved mode of operation, only the algorithms listed in Exhibit 13 and Exhibit 14 are available and the module transitions to the Non-Approved mode of operation whenever the algorithms listed in Exhibit 15 are invoked.

Upon receipt the Cryptographic Officer (CO) must perform the following steps to place, or ensure, that the module is operating in the FIPS Approved Mode:

1. Visually inspect the module to verify the hardware version is as listed above.
2. Power-up the module.
3. Run the Sanitize Command (CMD).
4. Load the FIPS Approved Firmware (FW) via the System Software Install Command CLI.
5. Power-cycle the module.
6. Login by entering the default password and then change it.
7. Run the Show Version CLI and verify the FW version is as listed above.
8. Run the Show Inventory CLI and verify the HW version is as listed above.
9. The CO must create the User role during initialization.
10. The module is now in FIPS Approved mode and will be after each subsequent power-cycle.

To switch from the FIPS Approved Mode of operation to the non-FIPS mode of operation perform the following steps:

1. Load the non-FIPS Firmware (FW) via the System Software Install Command CLI
2. Run the Zeroize Command (CMD)
3. Run the Sanitize Command (CMD)
4. Reboot the module
5. Install the non-FIPS License
6. Reboot the module

ACRONYMS

If applicable, specify any acronyms related to the cryptographic module that will be referenced in this document:

TERM	DESCRIPTION
CLI	Command Line Interface
CMD	Command
LED	Light Emitting Diode
AES	Advanced Encryption Standard

CSP	Critical Security Parameter
CO	Cryptographic Officer
SHA	Secure Hash Algorithm
CMVP	Cryptographic Module Validation Program

Exhibit 3 – *Specification of Acronyms and their Descriptions*

SECURITY LEVEL SPECIFICATION

The following are the security levels corresponding to each area:

SECURITY REQUIREMENTS AREA	LEVEL
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

Exhibit 4 – *Security Level Table.*

PHYSICAL PORTS AND LOGICAL INTERFACES

The Vcinity, Inc. RAD X-1040 AES-256 Cryptographic Module supports the following ports and logical interfaces:

PHYSICAL PORT	LOGICAL INTERFACE
System Power LED	Status Output
System Reset Switch	Control Input

Management Ethernet Speed/Activity LED	Status Output
Management Ethernet Link/Activity LED	Status Output
System Status LED	Status Output
InfiniBand Link LEDs	Status Output
40GE Link LED	Status Output
1/10GE Link LEDs	Status Output
QTY.2 4X InfiniBand FDR ports with pluggable QSFP+ optics	Data Input/Output
QTY.2 40Gbps Ethernet ports with pluggable QSFP+ optics	Data Input/Output
QTY.6 1G/10G Ethernet ports with pluggable SFP+ optics	Data Input/Output
QTY.1 10/100/1000Base-T Ethernet management port	N/A -Latent functionality; disabled for FIPS
QTY.1 RJ-45 RS-232 management console port	Control Input
QTY.1 USB 2.0 port	Control Input (firmware upgrade)
QTY.2 rear combined power supplies (each with its own AC Inlet) / fan modules.	Power

Exhibit 5 – *Specification of Cryptographic Module Physical Ports and Logical Interfaces*

The physical ports and logical interfaces are the same in the Approved and Non-Approved modes of operation.

SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

1. The module is considered to be operating in the FIPS Approved Mode of Operation when abiding by the security rules and requirements in the Security Policy. Any violation of the Security Policy will immediately place the module in a non-FIPS Approved Mode of Operation, and the module is not considered fit to protect sensitive but unclassified information.

2. The module only supports console access in the FIPS Approved Mode, ssh access is disabled.
3. The module inhibits data output when performing power-up self-tests; interfaces are not enabled until such a time that all power-up self-test pass.
4. The module inhibits data output when in the error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module does not support concurrent operators.
7. The module does not support private keys or key generation in the FIPS Approved Mode.
8. The module will clear results of previous authentications when it is power-cycled; operator shall be required to reauthenticate into the module before executing any authenticated services.
9. The module does not support feedback (e.g. echo) of authentication data during the authentication procedure.
10. The module supports a limited operational environment; it only loads and executes trusted code; signed by Vcinity, Inc. using HMAC SHA-512. As such, all of the FIPS 140-2 Area 6 requirements are not applicable.
11. The AES-GCM key shall be generated by an approved SP800-90A DRBG and then manually entered into the module. This will ensure the freshness of keys.
12. Operator shall not assign the same key to multiple interfaces; each interface (total of 128 possible) must be assigned a fresh key.
13. If a rolling reboot ensues, RMA the box. The operator is not allowed to switch image.
14. Using the function passwordHistory.get() the module can fetch the last N passwords (configurable via API authentication local password-history). There is no Max (2^32-1). Vcinity, Inc. recommends that this API to be called with “4” as the defined limit. This will ensure the operator does not attempt to re-use any of their last 4 passwords. The module cannot export the passwords from the boundary.
15. If the GCM IV counter has been exhausted, the session will abort. The operator must manually enter a new GCM key, which in turn will automatically reset the IV.
16. Upon completion of the power-on self tests, the module outputs the message “Vcinity RAD X Ready.”
17. On-demand self-tests are performed by power-cycling the module.
18. Upon failure of the power-on self-tests, the module enters the hard error state and outputs “[FAILED] Failed Self Test ______”, with the appropriate self-test inserted.
19. Upon failure of the firmware download test, the module enters the hard error state and outputs “IMAGE FAILED VALIDATION: ENTERING FAILURE STATE.”
20. Upon failure of the manual key entry test, the module enters the transient soft error state, outputs “No match.”, and allows the operator to start from the beginning and re-enter a fresh key.

21. The lockout duration upon 10 failed logins shall be set to at least 1 minute. The default lockout duration is 10 minutes. To set the lockout duration, the operator performs the command "authentication tally-failed-logins lockout-duration [time]"
22. The module is delivered in non-FIPS mode and may then be put in the FIPS Approved Mode by the operator. The module may be put back in the non-FIPS mode by the operator. However, after zeroization and returning to non-FIPS mode the module cannot be put back in the FIPS Approved Mode by an operator. The only method to return to the FIPS Approved Mode is to return the module to Vcinity via the RMA process.
23. When the module is in the non-FIPS mode of operation it does not have access to any Critical Security Parameters,
24. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS

CSP Name	Type	Generation	Establishment	Entry	Output	Storage	Key-To-Entity	Zeroization
Admin Password	8-128 bytes	N/A	N/A	Plaintext via console	N/A	Plaintext in Flash; Also in Ram during execution	This key belongs to the Crypto Officer	Zeroization in RAM is done via reboot; Zeroization in FLASH is done by the Zeroization service
User Password	8-128 bytes	N/A	N/A	Plaintext via console	N/A	Plaintext in Flash; Also in Ram during execution	This key belongs to the User	Zeroization in RAM is done via reboot; Zeroization in FLASH is done by the Zeroization service
AES-GCM Encryption Key	256 bits	N/A	N/A	Plaintext via console (Manual Transport/Electronic entry)	N/A	Plaintext in RAM; Plaintext in FLASH; Plaintext in FPGA	KEY_ID Table assigning a key per link	Zeroization in RAM is done via reboot; Zeroization in FLASH and FPGA is done by the Zeroization service
AES-GCM IV	96 bits	Deterministic construction per SP 800-38D 8.2.1 and IG A.5 Technique #3	N/A	Incoming plaintext over Optical Wire when performing GCM	Outgoing plaintext over Optical Wire, sent to the	Plaintext in FPGA	KEY_ID Table assigning an IV per link	Zeroization via Zeroization service

				Decryption for the client.	client to perform GCM Decryption.			
HMAC-SHA-512 Vcinity Firmware Key	256 bits	N/A	N/A	N/A – Injected during manufacturing	N/A	Plaintext in RAM; Plaintext in FLASH	FW integrity process	Zeroization is done via the Zeroization service

Exhibit 6 – *Table of CSPs, Public Keys, and Private Keys*

IDENTIFICATION AND AUTHENTICATION POLICY

The following is the list of roles and authentication available in the module:

ROLE	AUTHENTICATION TYPE	AUTHENTICATION DATA
Cryptographic Officer(Admin)	Role-based	Admin Password
User	Role-based	User Password

Exhibit 7 - *Roles and Required Identification and Authentication (FIPS 140-2 Table C1)*

The Cryptographic Officer (Admin) is defined as the Admin user that uses the admin password. The User is an operator that is created by the Admin user and assigned to any group of the module.

The module enforces the following password rules:

- Be at least 8 characters
- Be different from the current password by at least 4 characters
- Have at least one digit
- Have at least one uppercase letter
- Have at least one lowercase letter
- Have at least one non-letter/digit character
- Not be a palindrome
- Not be the current password with only a change of case
- Not be a rotated version of the current password
- Not be a word in the checker's dictionary

The module requires that the password be at least 8 characters, which is 64 bits. The default lockout duration after 10 consecutive attempts is 10 minutes. The operator must not set the lockout duration to shorter than 1 minute, enforced by policy. The strength of the authentication mechanism with multiple consecutive attempts in one minute is based upon the worst-case scenario of 1 minute as the lockout duration.

The strength of the authentication mechanism is as follows:

AUTHENTICATION MECHANISM	STRENGTH OF MECHANISM: MULTIPLE CONSECUTIVE ATTEMPTS IN A MINUTE	STRENGTH OF MECHANISM: SINGLE ATTEMPT
Password Verification	The operator is locked out for a minimum of 1 minute after 10 failed authentication attempts. Therefore the probability of success of multiple random guesses in 1 minute is 10/2^64.	The probability of success of a single guess is 1/2^64

Exhibit 8 - *Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)*

CRYPTOGRAPHIC MODULE SERVICES and ACCESS CONTROL

The following table indicates the authenticated services available to each role within the module in the approved modes of operation:

The access types are defined as follows: R: read; W: write; X: execute

Role		**Service**	**Cryptographic Keys & CSPs**	**Type(s) of Access**
Crypto-graphic Officer (Admin)	**User**			
X	X	Configure	N/A	N/A
X	X	Enable	N/A	N/A
X	X	Disable	N/A	N/A
X	X	End	N/A	N/A
X	X	Exit	N/A	N/A

X	X	No	N/A	N/A
X	X	Display/Reporting (Show Status)	N/A	N/A
X	X	System Configuration	HMAC-SHA-512 Vcinity Firmware Key	RX
X	X	System Environment	N/A	N/A
X	X	User Configuration	Admin Password User Password	RWX
X	X	Licensing	N/A	N/A
X	X	Network Interface	N/A	N/A
X	X	Crypto	AES-GCM Encryption Key AES-GCM IV	RWX
X	X	ACL	N/A	N/A
X	X	Zeroize	HMAC-SHA-512 Vcinity Firmware Key Admin Password User Password AES-GCM Encryption Key AES-GCM IV	W

Exhibit 9 – *Table of authenticated services in the Approved mode of operation*

The following table indicates the unauthenticated services available to the operator in the Approved mode of operation:

Service	**Cryptographic Keys & CSPs**	**Type(s) of Access**
Self-Test	HMAC-SHA-512 Vcinity Firmware Key	RX
LED viewing	N/A	N/A

Exhibit 10 – *Table of unauthenticated services in the Approved mode of operation*

The following table indicates the services available for each role in the Non-Approved mode of operation:

Role		Service	Non-Approved Algorithms Used
Cryptographic Officer	User		
X	X	Configure	N/A
X	X	Enable	N/A
X	X	Disable	N/A
X	X	End	N/A
X	X	Exit	N/A
X	X	No	N/A
X	X	Display/Reporting	SSHv2, ChaChaPoly
X	X	System Configuration	SSHv2, AES-128 (non-compliant), AES-256 (non-compliant), ChaChaPoly
X	X	System Environment	SSHv2
X	X	User Configuration	AES-128 (non-compliant), AES-256 (non-compliant), LDAP, TLS
X	X	Licensing	SSHv2, AES-256 (non-compliant)
X	X	Network Interface	AES-256 (non-compliant)
X	X	Crypto	AES-256 (non-compliant)
X	X	ACL	N/A
X	X	Zeroize	N/A

Exhibit 11 – *Table of authenticated services in the Non-Approved mode of operation*

The following table indicates the unauthenticated services available to the operator in the Non-Approved mode of operation:

Service

Self-Test
LED viewing

Exhibit 12 – *Table of unauthenticated services in the Non-Approved mode of operation*

ALGORITHMS

APPROVED ALGORITHMS

In the FIPS Approved mode of operation the module uses the following Approved cryptographic algorithms:

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTHS, CURVES, OR MODULI	USE
A934	AES	FIPS 197 SP 800-38A SP 800-38D	CTR[1], GCM	256 bits	Data Encryption/ Decryption
A911	HMAC	FIPS 198-1	HMAC-SHA-512	256 bits	Message Authentication
A911	SHS	FIPS 180-4	SHA-512		Message Digest

Exhibit 13 – *Table of Approved Algorithms*

The AES-GCM key shall be generated by an approved SP800-90A DRBG and then manually entered into the module. This will ensure the freshness of keys. The AES GCM IV generation is performed entirely deterministically per SP 800-38D Section 8.2.1 and IG A.5 Technique #3.

- The AES GCM IV is 96 bits. The IV is constructed of a randomly generated 32 bit name field that is used for the duration of the session and a 64 bit non-repetitive, incrementing counter.
- The 32 bit name field is constructed by adding a 32 bit random number to the module ID (name) assigned to the module.

[1] AES-CTR is only used as a prerequisite to AES-GCM.

- The 64 bit counter starts at zero and increments. When the counter reaches the maximum value of 2^{64}-1 the session is aborted.

The IV restoration is performed via option #3 – This is not enforced by the module; the operator is required to establish a new GCM Key upon power-cycle.

NON-APPROVED ALGORITHMS USED IN FIPS APROVED MODE

In the Approved mode of operation the module uses the following non-Approved but allowed algorithms:

ALGORITHM	USE
Vcinity, Inc. Proprietary SHA-512 (non-compliant) Obfuscation (no security claimed) as per IG 1.23	Obfuscation of the license file during entry; Obfuscation of passwords in Flash
Vcinity, Inc. Proprietary SHA-512 (non-compliant) Hash Verification (no security claimed) as per IG 1.23	Verification of the license file subsequent to entry; Verification of passwords in Flash
CRC-17 Verification as per IG 1.23	Producing Ingress/Egress statistics for CAM entry, hash table, packet drops.

Exhibit 14 – *Table of Non-Approved but Allowed Algorithms*

NON-APPROVED ALGORITHMS USED IN THE NON-FIPS MODE OF OPERATION

In the Non-Approved mode of operation the module uses the following Non-Approved cryptographic algorithms:

ALGORITHM	USE
AES-128 (non-compliant)	SNMP, SSH, HTTPS
AES-256 (non-compliant)	SSH, HTTPS, Data encryption/Decryption
chachaPoly	SSH
SSHv2	Remote login User Authentication
LDAP	User Authentication/Authorization

TLS	LDAP Certificate installation, HTTPS

Exhibit 15 – *Table of Non-Approved Algorithms Used in the Non-FIPS Mode of Operation*

SELF-TESTS

The module implements the following self-tests:

Power-up:

A. Firmware Integrity Test (HMAC-SHA-512)
B. Linux Kernel SHA-512 KAT
C. FPGA AES-GCM-256 Encrypt KAT
D. FPGA AES-GCM-256 Decrypt KAT
E. HMAC-SHA-512 KAT

Critical Function Tests: N/A

Conditional Test:

A. Continuous TRNG and DRBG tests: N/A
B. Pairwise tests: N/A
C. Duplicate Key Entry Test - Manual Key Entry Test (The module accepts keys through the console via HEX Input.)

D. FW Download Test (HMAC-SHA-512)

E. Bypass: N/A

Note: The AES-CTR is only used as a prerequisite to the AES-GCM implementation. Therefore, per IG 9.4 the vendor did not include separate AES-CTR KATs.

OPERATIONAL ENVIRONMENT

The module supports a limited operational environment; it only loads and executes trusted code signed by Vcinity, Inc. using HMAC SHA-512. As such, all of the FIPS 140-2 Area 6 requirements are not applicable.

PHYSICAL SECURITY POLICY

The module is designed and produced with commercially available production grade components. The module does not include any other physical security mechanisms.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

Exhibit 16 *Inspection/Testing of Physical Security Mechanisms*

MITIGATION OF OTHER ATTACKS POLICY

The module is not designed to mitigate any other attacks.

OTHER ATTACKS	MITIGATION MECHANISM	SPECIFIC LIMITATIONS
N/A	N/A	N/A

Exhibit 17 – *Table of Mitigation of Other Attacks (FIPS 140-2 Table C6)*