ACT2Lite Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 1.4

March 15, 2020

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Cisco's ACT2Lite Cryptographic Module, version 1.5. This security policy describes how the module meets the security requirements of FIPS 140-2 Level 2 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area 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	Electromagnetic Interface/Electromagnetic Compatibility	3
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**2**

Table 1 – Module Validation Level

1.3 References

This document deals only with operations and capabilities of the ACT2Lite Cryptographic Module listed above in section 1 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, ACT2Lite Cryptographic Module is also referred to as ACT2Lite or the module.

1.5 Document Organization

The Security Policy document is part of the 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

This document provides an overview of the ACT2Lite identified in section 1 above and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 ACT2Lite Module

ACT2Lite (Anti-Counterfeit Technology 2 Lite), version 1.5, is the ACT family (ACT 1T, Quack 1 and 2) next generation chip which is identified as 15-14497-02. The 15-14497-02 is an ancillary security device containing product identity information and assertion functionality to support product identity for various usages including anti-counterfeit functionality as well as other security functionality to be used across many different hardware platforms. It has been enhanced to provide 56 KB of EEPROM storage along with FIPS accepted cryptographic functions.

The ACT2Lite has CLIIP (Chip Level Identity Package) a SUDI (Secure Unique Device Identifier) certificate and a certificate chain (x.509v3 based on IEEE 802.1AR) inside the chip. This process occurs at manufacturing. Linking the installed certificates and the ACT-2 Lite chip provides the data needed to trace the chip from creation to completion of the Identity Insertion Process for assertion and reconciliation.

2.1 Cryptographic Module Characteristics

ACT2Lite is an opaque single-chip hardware module. Its function is primarily to provide a hardware anchored identity source through a globally unique and cryptographically assertable identity using public key cryptographic mechanisms and support for additional identities which can be similarly asserted. The assertion material (e.g. the private key) is kept within the physical confines of the ACT2Lite chip and is not allowed to leave that chip under any circumstances once the initial identity is installed. Subsequent identities require that the key pair be generated within the chip. The ACT2-Lite chip does not allow parallel capabilities. This means that only one cryptographic function/service can be executed at a time.

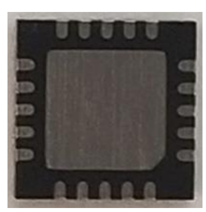

Image 1 – Bottom of ACT2Lite (15-14497-02)

Image 2 – Top of ACT2Lite (15-14497-02)

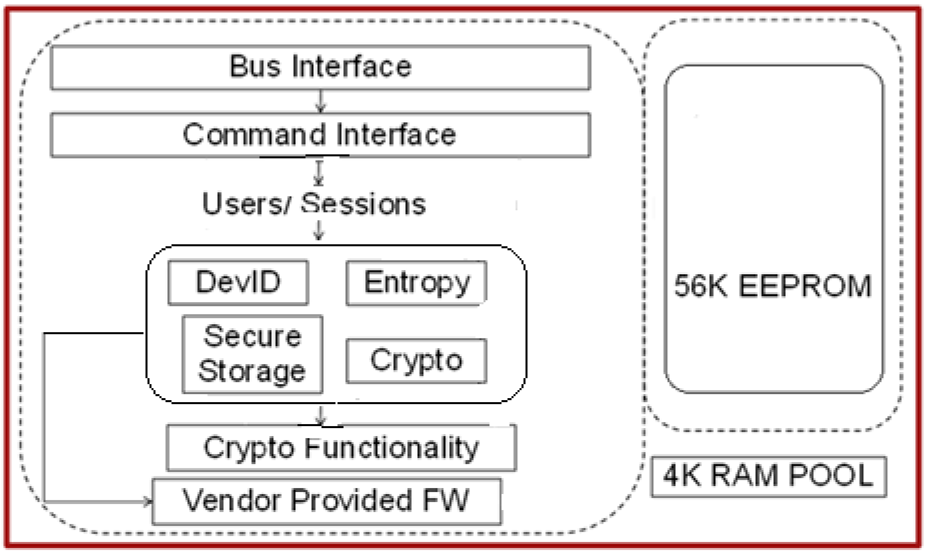

Figure 1 - Cisco ACT2Lite Logical block diagram

The module's logical block diagram is shown in Figure 1 above. The cryptographic boundary is the physical boundary of the module, which is the chip itself and all components contained within.

2.2 Module Interfaces

ACT2Lite cryptographic module support physical ports via 20 distinct pins, each with corresponding logical interfaces supported by the cryptographic module: data input, control input, data output and status output.

Interface	Description
Data Input	API input parameters over distinct pin
Data Output	API output parameters over distinct pin
Control Input	API input function calls over distinct pin
Status Output	API return status over distinct pin

Table 2 – Logical Interface Details

2.3 Roles and Services

The Module meets all FIPS 140-2 level 2 requirements for Roles and Services, implementing both Crypto Officer and User roles. Crypto Officer and User access to cryptographic services are Role-based.

The Crypto Officer UserID is 0x01 and the User UserID is also one byte, ranging from 0x02 to 0x0F. When the Crypto Officer and the User roles first initiate, a Password is generated and assigned to the perspective UserID. Then a session ID is generated and assigned to both the UserID and the Password.

The Password is tied to the UserID and kept in EPROM. If the Password matches, then there is a successful authentication. It must match prior to any crypto services being allowed by the perspective role. The Module does not allow concurrent operators.

The Crypto Officer password is the same as the User password in that both are 32-bytes long, but the CO password is generated differently than the User Role password. The host produces a 32-byte string. Which gets added to the chip generated 32-byte string. The 64-bytes gets hashed by SHA256 with 32-bytes being used as the CO password. In short, the strength of the password for the Crypto Officer would be considered the same as the User password yet multiple steps were used to produce the password.

The User passwords must each be at a minimum of 32 bytes long, each byte in the range 0x01 to 0xFE (inclusive). The probability of randomly guessing the correct sequence is $1/254^{32}$ which is less than 1/1,000,000. The average number probability of guesses required to guess the correct sequence is 254^{32}, so in order to guess the password in a 1-minute period it would require, on average, as many guesses. To achieve a probability less than 1/100,000 of guessing the sequence, the system would have to be able to make 254^{32} / 100,000 guesses in one minute, which is well beyond the capabilities of the device.

The services available to the Crypto Officer and User roles consist of the following:

Services	Access	CSPs	Crypto Officer	User
Random number generator instantiation/reseed	execute	DRBG entropy input, DRBG seed, DRBG V and DRBG key	**X**	

Set User	execute	N/A	**X**	
Zeroization	Execute	DRBG entropy input, DRBG seed, DRBG V, DRBG key, symmetric keys, asymmetric public keys, asymmetric private keys and HMAC keys	**X**	
ECDSA Signature generation	Execute/Write (for Crypto Officer Only)	Asymmetric private keys	**X**	**X**
ECDSA Signature verification	execute/Write (for Crypto Officer Only)	Asymmetric public keys	**X**	**X**
AES Encryption/decryption	execute/Write (for Crypto Officer Only)	Symmetric Keys	**X**	**X**
Perform Self-Tests	execute/read	N/A	**X**	**X**
Power	execute	N/A	**X**	**X**
RSA Signature generation	execute/Write (for Crypto Officer Only)	Asymmetric private keys	**X**	**X**
RSA signature verification	execute/Write (for Crypto Officer Only)	Asymmetric public keys	**X**	**X**
Show Status	Execute/read	N/A	**X**	**X**

Table 3 - Services

2.4 Physical Security

The module obtains its physical security from silicon nitride, a white, high-melting-point solid that is relatively chemically inert and very hard (8.5 on the mohs scale). It has a high thermal stability.

2.5 Cryptographic Key Management

Keys reside in internally allocated data structures and can only be accessed using the Module defined API. The operating system protects memory and process space from unauthorized access. Zeroization of sensitive data is performed automatically by API function calls for intermediate data items.

The module supports the following keys and critical security parameters (CSPs):

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES 256)	384-bits	This is the entropy for SP 800-90A CTR_DRBG. Software based entropy source used to construct seed.	RAM (plaintext)	Zeroized upon zeroize API call or Power cycle the module
DRBG Seed	SP800-90A CTR_DRBG (AES 256)	384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input.	RAM (plaintext)	Zeroized upon zeroize API call or Power cycle the module
DRBG V	SP800-90A CTR_DRBG (AES 256)	128-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function.	RAM (plaintext)	Zeroized upon zeroize API call or Power cycle the module
DRBG Key	SP800-90A CTR_DRBG (AES 256)	256-bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	RAM (plaintext)	Zeroized upon zeroize API call or Power cycle the module
Symmetric Keys	AES	128, 192, 256 bits.	AES: 128, 192, 256 bits. Generated by calling approved SP800-90a DRBG	EEPROM	Zeroized upon zeroize API call
Message authentication	HMAC	HMAC-SHA-1/256/384/512	Generated by calling approved SP800-90a DRBG.	EEPROM	Zeroized upon zeroize API call
RSA Private Key	RSA	2048 bits	Derived from asymmetric algorithm (RSA/ECDSA) standard.	EEPROM (plaintext)	Zeroized upon zeroize API call
RSA Public Key	RSA	2048 bits	Derived from asymmetric algorithm (RSA/ECDSA) standard.	EEPROM (plaintext)	Zeroized upon zeroize API call
ECDSA private key	ECDSA	Curves: P-256,384,521	Derived from asymmetric algorithm (RSA/ECDSA) standard.	EEPROM (plaintext)	Zeroized upon zeroize API call
ECDSA public key	ECDSA	Curves: P-256,384,521	Derived from asymmetric algorithm (RSA/ECDSA) standard.	EEPROM (plaintext)	Zeroized upon zeroize API call
Operator password	Password	32 characters	The password of the Crypto Officer and User roles. This CSP is generated internally.	EEPROM (plaintext)	Zeroized when Operator is deleted.

Table 4 -Cryptographic Keys and CSPs

2.6 Cryptographic Algorithms

Approved Cryptographic Algorithms

The cryptographic module supports the following FIPS-140-2 approved algorithm implementations:

Algorithm	CAVP Certificate Number
AES (128/192/256 bits CBC, ECB, 256 bit CTR)	2556
HMAC (SHA-1/256/384/512)	1576
SHS (SHA-1/256/384/512)	2156
RSA (KeyGen, SigGen and SigVer; PKCS1_V1_5; 2048bits with SHA-1/256/384/512)	1309
ECDSA (KeyGen, SigGen and SigVer; P-256 with SHA-256/384/512, P-384 with SHA-384/512, P-521 with SHA-512)	439
CTR_DRBG (AES-256)	384

Table 5 – Approved Algorithms

Notes:

- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

Non-FIPS Approved But Allowed Cryptographic Algorithm

- NDRNG

2.7 Self-Tests

The modules include an array of self-tests that are run automatically during startup and periodically when called during operations to prevent any secure data from being released and to insure all components are functioning correctly.

Self-tests performed

- Power On Self-Tests (POSTS)
    - AES ECB and CBC (encrypt/decrypt) KATs
    - DRBG KAT (SP800-90A Health Tests)
    - ECDSA KAT (separate KAT for signing; separate KAT for verification)
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - RSA KAT (separate KAT for signing; separate KAT for verification)

- Conditional tests
    - Continuous random number generation test for SP800-90A DRBG
    - Continuous random number generation test for NDRNG
    - Pairwise consistency test for ECDSA
    - Pairwise consistency test for RSA

The module inhibits all access to cryptographic algorithms and self-tests due to the process architecture in use. The power-on self-tests are performed after the system is initialized but prior to the underlying OS initialization which prevents the security appliances from operating. In the event of a power-on self-test failure, the cryptographic module will force the platform to reload and reinitialize cryptographic module. When self-tests fail the module does not allow any commands to be process. A status inquire command will also provide failure status information.

In addition to the automatic operation at cryptographic module initialization time, self-tests can also be initiated on demand by the Crypto Officer or User.

3 Secure Operation of the ACT2Lite

The module is completely and permanently embedded into its associate hardware chip. Making it impossible to edit, delete or copy. Once the Host is powered up and the module completes its self-test the module is in FIPS mode and remains in FIPS mode until powered down.

The Module functions entirely within the process space of the process that invokes it, and thus satisfies the FIPS 140-2 requirement for a single user mode of operation.

The following policy must always be followed in order to achieve a FIPS 140-2 mode of operation:

- Calling the function ACT-2Lite_init() initializes the cryptographic module, and places the module in the FIPS-approved mode of operation.

- Only FIPS approved or allowed algorithms and key sizes may be used. Please refer to section 2.6 for more information.

Upon power-up of the Module, the module will run its power-up self-tests. Successful completion of the power-up self-tests indicates the module has passed the self-tests and is ready within the Host.