ACT2Lite Module

FIPS 140-2 Non Proprietary Security Policy

Level 1 Validation

Version 0.1

September 22, 2015

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Cisco's ACT2Lite Module, Version 1.5. This security policy describes how the module meets the security requirements of FIPS 140-2 Level 1 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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	3
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 - Module Validation Level

1.3 References

This document deals only with operations and capabilities of the ACT2Lite 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 Module is referred to as ACT2Lite, A2L 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, version 1.5 (Anti-Counterfeit Technology 2 Lite) is the ACT family (ACT 1T, Quack 1 and 2) next generation chip. They are identified singularly as 15-14497-02 which comprises either 15-14497-02(NX315), 15-14497-02(AT90S072) or 15-14497-02(NDS_ACT2_V1). The chip 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 A2L 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

A2L 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 A2L 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. All processing is done on either a 15-14497-02(AT90S072) secure 8/16 bit low power RISC CPU, a 15-14497-02(NX315)secure 16-bit microcomputer or a 15-14497-02(NDS_ACT2_V1) secure 35 MHz, 32-bit processor.

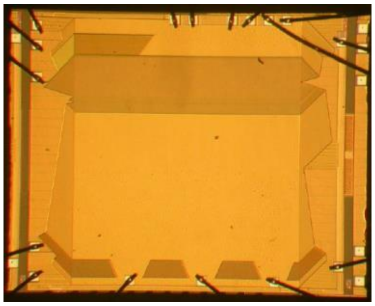

Image 1 - 15-14497-02(NX315), 15-14497-02(AT90S072) or 15-14497-02(NDS_ACT2_V1)

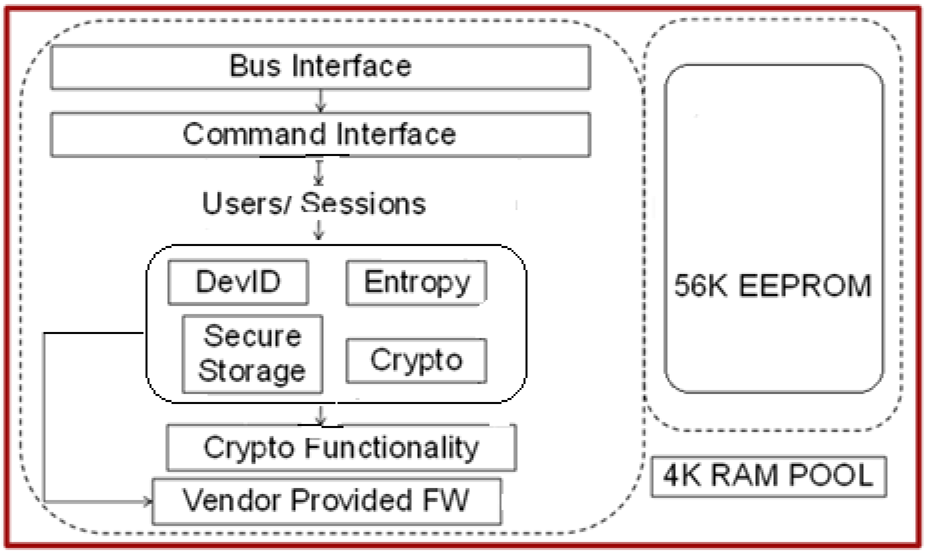

Figure 2 - Cisco ACT2Lite Logical block diagram

The module's logical block diagram is shown in Figure 1 above. The cryptographic boundary is the physical boundary of the module, which contains all components.

2.2 Module Interfaces

A2L 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 Interfaces Details

2.3 Roles and Services

The Module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both Crypto Officer and User roles, which are classed as processes. Once a role initially logs onto the module it is assigned a unique number. These values must match prior to any crypto functions being allowed by the perspective role. The Module does not allow concurrent operators.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Module.

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	Asymmetric private keys	X	X
ECDSA Signature verification	execute	Asymmetric public keys	X	X
AES Encryption/decryption	execute	Symmetric Keys	X	X
Perform Self-Tests	execute/read	N/A	X	X
Power	execute	N/A	X	X
RSA Signature generation	execute	Asymmetric private keys	X	X
RSA signature verification	execute	Asymmetric public keys	X	X
Show Status	execute	N/A	X	X

Table 3 – Services

2.4 Physical Security

The module obtains its physical security from any installed platform with production grade components as allowed by FIPS 140-2 level 1.

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):

Key/CSP Name	Services	Description	Storage and Zeroization
DRBG entropy input	Random number generator	Entropy for SP 800-90A DRBG. HW based entropy source output used to construct DRBG seed.	Stored in RAM in plaintext; Zeroized upon zeroize API call or Power cycle the module.
DRBG seed	Random number generator	Seed for SP 800-90A DRBG. Input to the DRBG that determines the internal state of the DRBG.	Stored in RAM in plaintext; Zeroized upon zeroize API call or Power cycle the module
DRBG V	Random number generator	Internal V value for SP 800-90A DRBG. Generated by entropy source via the CTR_DRBG derivation function.	Stored in RAM in plaintext; Zeroized upon zeroize API call or Power cycle the module
DRBG key	Random number generator	Internal key for SP 800-90A DRBG. Generated from entropy source via CTR_DRBG derivation function	Stored in RAM in plaintext; Zeroized upon zeroize API call or Power cycle the module
Symmetric Keys	Encryption/ decryption	AES: 128, 192, 256 bits. Generated by calling approved SP800-90a DRBG	Stored in EEPROM in plaintext; Zeroized upon zeroize API call
Asymmetric private keys	Signature generation	RSA: 2048 bits; ECDSA: P-256, P-384 and P-521. Generated by calling approved SP800-90A DRBG.	Stored in EEPROM in plaintext; Zeroized upon zeroize API call
Asymmetric public keys	signature verification	RSA: 2048 bits; ECDSA: P-256, P-384 and P-521. Derived from asymmetric algorithm (RSA/ECDSA) standard.	Stored in EEPROM in plaintext; Zeroized upon zeroize API call
HMAC Keys	Message authentication	Used for HMAC-SHA-1/256/384/512. Generated by calling approved SP800-90a DRBG.	Stored in EEPROM in plaintext; Zeroized upon zeroize API call

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	Algorithm Certificate Number
AES	2556
HMAC	1576
SHS	2156
RSA	1309
ECDSA	439
DRBG	384

Table 5 - Approved Cryptographic Algorithms for 15-14497-02(AT90S072)

Algorithm	Algorithm Certificate Number
AES	2742
HMAC	1719
SHS	2314
RSA	1438
ECDSA	480
DRBG	461

Table 6 - Approved Cryptographic Algorithms for **15-14497-02(NX315)**

Algorithm	Algorithm Certificate Number
AES	3002
HMAC	1899
SHS	2513
RSA	1570
ECDSA	550
DRBG	572

Table 7 - Approved Cryptographic Algorithms for 15-14497-02(NDS_ACT2_V1)

Notes:

- RSA (Cert. #1309; non-compliant with the functions from the CAVP Historical RSA List)
  - FIPS186-4:
    ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(1))

- RSA (Cert. #1438; non-compliant with the functions from the CAVP Historical RSA List)
  - FIPS186-4:
    ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(1))

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 (encrypt/decrypt) KATs
  - DRBG KAT
  - ECDSA KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - RSA KAT

- 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. If an error occurs during the self-test the module outputs the following message:

requesting a reload of the OS. %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed **(**<*failing test description*>**)** where <*failing test description*> identifies the name of the self-test that failed.