



**FIPS 140-2 Non-Proprietary Security
Policy for
INTEGRITY Security Services
High Assurance Embedded Cryptographic
Toolkit**

Module Version 3.0.3

Document Version 3.0.6



7585 Irvine Center Drive
Suite 250
Irvine, CA 92618
USA
Tel: 949-756-0690
Fax: 949-756-0691
www.ghs.com

DISCLAIMER

GREEN HILLS SOFTWARE, INC., MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. Further, Green Hills Software, reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Green Hills Software, to notify any person of such revision or changes.

Green Hills, the Green Hills logo, CodeBalance, GMART, GSTART, Slingshot, INTEGRITY, and MULTI are registered trademarks of Green Hills Software, Inc. AdaMULTI, Built With INTEGRITY, EventAnalyzer, G-Cover, GHnet, GHnetLite, Green Hills Probe, Integrate, ISIM, PathAnalyzer, Quick Start, ResourceAnalyzer, Safety Critical Products, SuperTrace Probe, TimeMachine, TotalDeveloper, velOSity, and μ -velOSity are trademarks of Green Hills Software, Inc. All other company, product, or service names mentioned in this book may be trademarks or service marks of their respective owners.

ISS ECT FIPS 140-2 Security Policy

PubID: ISS ECT-SP-006

Version: 3.0.3

November 2016

Table of Contents

1	Introduction	5
1.1	Audience	5
1.2	Document Purpose	6
1.3	Additional Information.....	6
1.4	ISS HA-ECT API.....	6
2	Module Specification	7
2.1	The ISS HA-ECT FIPS Object Module	10
2.1.1	Integrity Validation Data	10
2.1.2	Exclusivity of Integrity Tests.....	10
2.1.3	Run-time Integrity Validation.....	11
2.2	Ports and Interfaces	12
2.3	Approved and Allowed Cryptographic Algorithms	13
2.3.1	Non-Approved but Allowed Cryptographic Algorithms.....	13
2.4	Approved Mode of Operation.....	15
2.4.1	Rules of Operation	15
2.5	Test Environment.....	16
3	Roles, Services, and Authentication.....	17
3.1	Roles and Services.....	17
3.2	Authentication	17
3.3	Authorized Services.....	18
4	Operational Environment	20
4.1	Compatible Platforms	20
4.2	Firmware Security	21
4.3	Self-Tests.....	22
4.3.1	Power-up Self-Tests	23
4.3.2	Conditional Self-Tests	23
4.3.3	Critical Function Tests	23

4.3.4	Physical Security.....	23
4.3.5	Mitigation of Other Attacks	23
5	Design Assurance	24
5.1	Source Code Control	24
5.2	Application Management of Keys and Critical Security Parameters (CSPs)	24
	Keys and Critical Security Parameters (CSPs).....	24
	Identifying Keys and CSPs	25
	Key Generation	25
	Storage of Keys and CSPs	26
	Destruction of Keys and CSPs.....	26
	Entropy.....	26
6	Glossary.....	27
7	References	28
	Appendix A – Installation, Validation and Initialization.....	29

Chapter 1

1 Introduction

This document is the Non-Proprietary FIPS 140-2 Security Policy for the Green Hills Software INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit v3.0.3 to meet FIPS 140-2 Level 1 requirements. This Security Policy details the secure operation of the Green Hills Software INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit module, libect, as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

In this document, the Green Hills Software INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit module is referred to as the *Module*, or *ISS HA-ECT* or *ISS HA-ECT FIPS Object Module*.

1.1 Audience

This document is required as a part of the FIPS 140-2 validation process. It describes the ISS HA-ECT FIPS Object Module in relation to FIPS 140-2 requirements. The companion document

HA-ECT API Guide is a technical reference for operators using, and system administrators installing, the ISS HA-ECT FIPS Object Module, for use in risk assessment reviews by security auditors, and as a summary and overview for program managers.

1.2 Document Purpose

This Security Policy document is available in Green Hills Software ISS HA-ECT distributions.

This document outlines the functionality provided by the Module and gives high level details on the means by which the Module satisfies FIPS 140-2 requirements.

1.3 Additional Information

For more information on the ISS HA-ECT please contact support-iss@ghs.com. For more information on NIST and the cryptographic module validation program, please visit <http://csrc.nist.gov/groups/STM/cmvp/index.html>.

1.4 ISS HA-ECT API

The ISS HA-ECT FIPS Shared Object Module, libect, is designed as a complete crypto library. Applications can use the FIPS validated cryptographic functions of libect as a shared object library from applications as needed and calling the appropriate ISS HA-ECT API functions directly.

Chapter 2

2 Module Specification

For the purposes of FIPS 140-2 validation, the ISS HA-ECT FIPS Object Module v3.0.3 is defined as a specific discrete unit of binary object code generated from a specific source configuration owned and managed by Green Hills Software. The Module object code is created by Green Hills Software and placed into a library format appropriate for numerous operating systems. The binary version of this Module is suitable for a specific CPU architecture family. The binary version can be reproduced on demand by Green Hills Software by using its configuration management system (CM) which contains specific tags to track each validated Module. The Module provides a cryptographic API (Application Programming Interface) to external applications.

The Module is distributed as a firmware object, libect.a

The term Module elsewhere in this document refers to this ISS HA-ECT FIPS Object Module. For FIPS 140-2 purposes, the Module is classified as a multiple-chip embedded module.

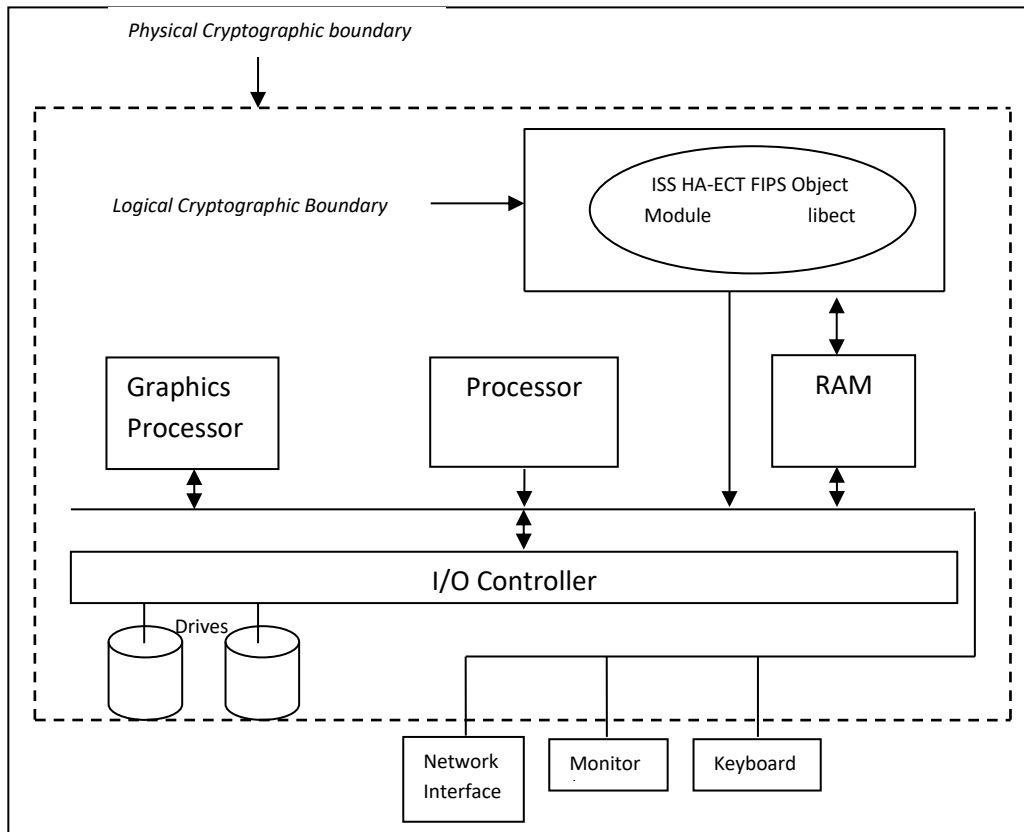


Figure 1 – Physical/Logical Cryptographic Boundary

The *physical* cryptographic boundary of the Module is the enclosure of the general-purpose computing system on which it is executing with the *logical* cryptographic boundary of the Module is the ISS HA-ECT FIPS Object Module (Figure 1). The Module performs no communications other than with the process that calls it. It makes no network or interprocess connections and creates no files.

One instance of the Module was tested by the FIPS 140-2 Cryptographic Module Testing (CMT) laboratory for the specific platforms:

Silicon Labs EM3581 ARM Cortex-M3

Development tools used by CMT to build for the target platform were:

IAR v7.40.1.8472
Target: Firmware
Binary: libect.a

The ISS HA-ECT FIPS Object Module, when generated from the identical unmodified source code, are “Vendor Affirmed” to be FIPS 140-2 compliant when running on other supported computer systems provided the conditions described in “Operational Environment”, are met. On any platform, the Module is not considered FIPS 140-2 validated if the binary’s integrity is not verified to match the known validated values listed in this Security Policy document.

The Module was designed and implemented to meet FIPS 140-2 requirements. In order to ensure FIPS 140-2 validated behavior, after linking, loading, and initializing the ISS HA-ECT FIPS Object Module within a runtime executable application, it is required that all rules and procedures listed in this Security Policy be followed by the operator at all times while the Module operates in FIPS-mode.

The process of generating the runtime application from ISS HA-ECT FIPS Object Module is the same for all platforms and is documented in the ISS HA-ECT API Guide. The Module provides confidentiality, integrity, and message digest services. It natively supports the following algorithms: AES-GCM, AES-CCM, AES-ECB, AES-CBC, AES-CTR DRBG, SHA-256, ECDSA, HMAC-SHA-256, as well as ECDH.

2.1 The ISS HA-ECT FIPS Object Module

Since the Module is distributed as prebuilt binary code, the integrity of the Module and executables which incorporate the Module is accomplished with a simple HMAC-SHA-256 digest verification.

2.1.1 Integrity Validation Data

The ISS HA-ECT FIPS Object Module file is protected by a HMAC-SHA-256 digest. This digest protects only object code belonging to the Module. The ISS HA-ECT FIPS Object Module is built from a set of object files linked into a single relocatable object file. This monolithic object file may be incorporated into a runtime executable application files, but in any event must be incorporated intact and in its entirety in order to operate in a FIPS 140-2 compliant mode. The module runs along with other application code in a non-modifiable environment.

Upon delivery, the system operator runs a Green Hills supplied utility program- ghash which using a FIPS validated crypto library (i.e this library), computes and displays the HMAC-SHA-256 digests for the Module. The ghash utility is used to compute the ghash and store the final libect library by Green Hills Software. These digests are recomputed, and verified at run-time to match the ghash-inserted values. The operator must provide assurance that the FIPS Object is not tampered with during the development process.

The ISS HA-ECT FIPS Object Module is carefully isolated from all other application object code. This isolation is accomplished by collecting all of the ISS HA-ECT FIPS Object Module code and data into reserved, specially named program sections. These two sections and their contents are as follows:

- .ecttext: ISS HA-ECT FIPS Object Module executable code
- .ectrodata: ISS HA-ECT FIPS Object Module constant/read-only data

The ISS HA-ECT FIPS Object Module contains only the contents of these two fixed sections. The integrity of the ISS HA-ECT FIPS Object Module file is protected by two HMAC-SHA-256 digests, one for each of these contiguous program sections. The HMAC-SHA-256 digests are computed using the ghash utility and stored in another special read-only data section, .ecthash. This section also contains the reference points (address range) corresponding to the hash values. These reference points ensure that the run-time digest is computed over exactly the same memory that is used at build-time.

2.1.2 Exclusivity of Integrity Tests

Standard object file dump utilities can be used to verify that the ISS HA-ECT FIPS Object Module contains no other code/data other than what is found in the specially named sections.

User application code is always placed into sections (e.g. .text, .data) that are not these special reserved sections. The operator can easily verify that the size of the special named FIPS sections are the same in the FIPS validated re-locatable Module as in the final executable. Therefore, no other memory is included in the HMAC_SHA256 validation.

2.1.3 Run-time Integrity Validation

When the ISS HA-ECT FIPS Object Module is initialized at run-time, the HMAC_SHA-256 digests are computed dynamically for all two sections and then compared against the constant values stored in the .ecthash section. The HA-ECT FIPS Module self-tests can also be executed during normal program operation. This can be useful for periodic health tests to ensure that the ISS HA-ECT FIPS Object Module executable and read-only data (e.g. algorithm constants in tables) have not been corrupted relative to their build-time values

2.2 Ports and Interfaces

For the purposes of this FIPS 140-2 validation, the Module is considered to be a multiple-chip embedded module. Although the Module is firmware, the physical embodiment is a computing platform that consists of multiple components considered to be a multichip embedded module by FIPS 140-2.

The logical cryptographic boundary for the Module is the discrete contiguous block of object code (the ISS HA-ECT FIPS Object Module) containing the machine instructions and data generated from the ISS HA-ECT FIPS source, as used by the calling application. The physical cryptographic boundary contains the computing hardware of the system executing the application. This system hardware includes the central processing unit(s), cache and main memory (RAM), system bus, and peripherals including disk drives and other permanent mass storage devices, network interface cards, keyboard and console and any terminal devices.

The Module provides a logical interface via an Application Programming Interface (API). This logical interface exposes services that applications may utilize directly or extend to add support for new data sources or protocols. The API provides functions that may be called by the referencing application.

The API interface provided by the Module is mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. Each of the FIPS 140-2 logical interfaces relates to the Module's callable interface, as follows:

- Data input: input parameters to all API functions that accept input from Crypto-Officer or User entities
- Data output: output parameters from all API functions that return data as arguments or return values from Crypto-Officer or User entities
- Control input: all API function input into the by the Crypto-Officer and User entities
- Status output: API information returned via return/exit codes to Crypto-Officer or User entities

The API function specifications are included in the ISS HA-ECT project documentation which covers both FIPS-approved, and non-FIPS-approved but allowed functions.

2.3 Approved and Allowed Cryptographic Algorithms

The Module supports the following FIPS-approved cryptographic algorithms:

- Advanced Encryption Standard (FIPS 197)
- CCM Mode for Authentication and Confidentiality (FIPS SP 800-38C)
- Secure Hashing Algorithm (SHA-256: FIPS 180-4)
- Keyed-Hash Message Authentication Code (HMAC: FIPS 198)
- Random Number Generator (DRBG: NIST SP 800-90A)
- Elliptic Curve Digital Signature Algorithm (ECDSA FIPS 186-4)

Algorithm Type	Algorithm	Validation Certificate	Use
Asymmetric keys	FIPS 186-4 ECDSA Public Key Generation using P-256 curve	#981	Sign, Verify, key pair generation operations
	FIPS 186-4 ECDSA Signature Verification Component using P-256 curve		
	FIPS 186-4 ECDSA Signature Generation Component using P-256 curve		
Symmetric keys	AES with modes CBC, ECB, CTR - each with 128, 192, or 256-bit keys	#4239	Encrypt/Decrypt operations
	AES GCM with 128, 192, or 256-bit keys		
	AES CCM with 128, 192, or 256-bit keys		
HMAC	HMAC-SHA-256 with key lengths greater than or equal to 112-bits	#2778	Firmware and Message Integrity and Authenticity
Hashing	SHA-256	#3477	Hashing
DRBG	SP 800-90A CTR DRBG using AES 128, 192, 256-bit	#1319	Random Number Generations

2.3.1 Non-Approved but Allowed Cryptographic Algorithms

The Module supports the following cryptographic algorithms:

- Pairwise Key Establishment Schemes (ECDH: FIPS SP 800-56A Revision 2)

Algorithm Type	Algorithm	Validation Certificate	Use
Key Exchange Primitives	Elliptic-Curve Diffie-Hellman	Non-Approved. Allowed in FIPS-mode	Used to compute key agreement primitives.

2.4 Approved Mode of Operation

The module always operates in the Approved Mode of Operation when initialized as described.

2.4.1 Rules of Operation

- The operator shall not make any changes to the Module's code while building an application.
- Only the HMAC-SHA-256 verified libect should be used without any modifications for a FIPS 140-2 compliant operation.
- The Module is initialized in the FIPS mode of operation (see Appendix A).
- The replacement or modification of the Module by unauthorized intruders is prohibited. The Operating System enforces authentication method(s) to prevent unauthorized access to Module services.
- All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.
- The referencing application accessing the Module runs in a separate virtual address space with a separate copy of the executable code.
- The unauthorized reading, writing, or modification of the address space of the Module is prohibited.
- The writable memory areas of the Module (data and stack segments) are accessible only by a single application so that the Module is in "single user" mode, i.e. only the one application has access to that instance of the Module.
- The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the Module.
- Across the power cycles, a human operator must reset the IV to the previously used IV.

2.5 Test Environment

The Module was tested by the FIPS 140-2 CMT laboratory on the following computer systems:

Silicon Labs EM3581 ARM Cortex-M3

Development tools used by CMT to build for the target platform were:

IAR v7.40.1.8472

Target: Firmware

Binary: libect.a

The ISS HA-ECT FIPS binary Object Module is “Vendor Affirmed” to be FIPS 140-2 compliant when running on other supported computer systems provided the conditions described in “Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program”, are met.

Chapter 3

3 Roles, Services, and Authentication

3.1 Roles and Services

The Module meets the FIPS 140-2 level 1 requirements for Roles and Services for User role and Crypto-Officer role.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented in the Module. The Crypto Officer role can install, initialize and remove the Module; this role is implicitly assumed while installing the Module or initializing the FIPS-mode on the Module.

Role	Authorized Services
User Role	Access to all services (loading Module, calling API's) except installation and FIPS-mode initialization
Crypto Officer role	Module install and FIPS-mode initialization Uninstalling or removing the Module

3.2 Authentication

As allowed by FIPS 140-2, the Module does not support user identification or authentication for those roles. Only one role may be active at a time and the Module does not allow concurrent operators. The Module does not provide identification or authentication mechanisms that would distinguish between the two supported roles. These roles are implicitly assumed by the services that are accessed, and can be differentiated by assigning module installation and configuration services to the Crypto Officer.

3.3 Authorized Services

The services provided by the Module are listed in the following table. All services may be performed in User role with the exception of Module installation and Initialization services which are the only services performed in the Crypto Officer role:

Service	Role	Critical Security Parameters	Algorithm	API Functions	Access
Symmetric Encryption/Decryption	User	Symmetric Key	AES	IclAES_Init, IclAES_ProcessBytes, IclAES_Finish, IclAESGCM_Init, IclAESGCM_AADUpdate IclAESGCM_AuthEncryptUpdate IclAESGCM_AuthDecryptUpdate IclAESGCM_Finish IclAESCCM_Init IclAESCCM_AuthEncrypt IclAESCCM_AuthDecrypt IclAESCCM_Finish ICL_AES_ECB_ENCRYPT, ICL_AES_ECB_DECRYPT, ICL_AES_CBC_ENCRYPT, ICL_AES_CBC_DECRYPT, ICL_AES_CBC_HASH, ICL_AES_CTR.	Read Write execute
Digital Signature	User	Asymmetric private key	ECDSA	IclECC_CalcPublicKey, IclECC_GenerateKey, IclECC_InitPoint, IclECC_IsValidKey, IclECDSA_Sign, IclECDSA_SignFromHash, IclECDSA_Verify, IclECDSA_VerifyFromHash	Read, Write, Execute
Message Digest	User	HMAC key	SHA-256 HMAC	IclHash_Finish, IclSHA256_Finish,, IclHash_HashBytes, IclSHA256_HashBytes, IclHash_Init, IclHash_Update, IclHMAC_Auth, IclHMAC_Finish, IclHMAC_Init, IclHMAC_SHA256_Auth, IclHMAC_Update	Read, Write, Execute
Random Number Generation	User	DRBG State	SP800-90A	IclRand, IclReseed	Read Write Execute
Show Status	User	None	N/A	ect_CurrentFIPSState	None
Module Install and Initialization	Crypto Officer	HMAC-SHA-256 Integrity Key	N/A	ect_EnableFIPSMode()	Read Execute

Service	Role	Critical Security Parameters	Algorithm	API Functions	Access
Uninstalling or removing the module	Crypto-Officer	None	None	None	None
Perform Power-up Self-Tests	User	HMAC-SHA-256 Integrity Key	N/A	ect_DoSelfTest	Read Execute
Key Establishment ¹	User	Asymmetric public and private keys	ECDH	IclECDH_CalcSharedSecret, IclECDH_GetPublicKey, IclECDH_Init	Read Write Execute
Zeroization	User	Asymmetric and symmetric keys	ECC ECDSA AES HMAC DRBG	IclECC_DestroyKeys, IclHMAC_Finish, IclAES_Finish, IclFinish	Read Zeroize
Big Number Operations	User	None		IclBigNum_Add, IclBigNum_AddUInt, IclBigNum_Assign, IclBigNum_Cmp, IclBigNum_CmpUInt, IclBigNum_DivMod, IclBigNum_ModMulInv, IclBigNum_Mul, IclBigNum_Pack, IclBigNum_Sub, IclBigNum_SubUInt, IclBigNum_Unpack, IclBigNum_ZeroExtend,	None

¹ This service does not establish a key in the Module; rather, it is used by the calling application as part of a system level key establishment scheme.

Chapter 4

4 Operational Environment

The ISS HA-ECT FIPS Object Module is generated from source code available for use on a wide variety of computer hardware and operating system platforms. Applications referencing the ISS HA-ECT FIPS Object Module run as processes under the control of the host system operating system. Modern operating systems segregate running processes into virtual memory areas that are logically separated from all other processes by the operating system and CPU. NOTE: in some simple computer systems (sometimes running on microprocessors without memory protection hardware as with FreeRTOS), the ISS HA-ECT FIPS Object Module necessarily is linked together in the same memory space as the other application code. However, the ISS HA-ECT FIPS Object Module was primarily designed for modern computer systems that provide process protection.

The ISS HA-ECT FIPS Object Module functions completely within the process space of the process which loads it. The Module does not communicate with any processes other than the one that loads it, and satisfies the FIPS 140-2 requirement for a single user mode of operation.

The ISS HA-ECT FIPS Object Module was tested on specific hardware/firmware environments. As stated in section G.5 of the “Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program”, the binary Module maintains FIPS 140-2 validation on other hardware and operating systems which were not included as part of the validation testing and without retesting the cryptographic Module on the new OS(s) and/or GPC(s). However, the CMVP makes no statement as to the correct operation of the Module when executed on an OS(s) and/or GPC(s) not listed on the validation certificate. The Module validated by the CMVP and which assurance is provided is based as caveated on the validation certificate and operated on the reference operating systems annotated on the certificate.

4.1 Compatible Platforms

The Module is designed to run on a very wide range of hardware and firmware platforms as long as the conditions in FIPS 140-2 Implementation Guidance G.5 are met. Any such computing platform that meets the conditions listed above can be used to host a FIPS 140-2 validated Module generated in accordance with this Security Policy. Such use will be considered “vendor-affirmed” for platforms other than those used for FIPS 140-2 testing as specified in this Security Policy.

If any platform specific errors occur that can only be corrected by modification of the Module source files, then the Module will not be validated for that platform. Note also that future releases of ISS HA-ECT may add support for additional platforms requiring new platform specific source replacing parts of the source corresponding to the current validated Module, in which case the modified Module will require revalidation under FIPS/NIST guidelines.

Note there is a possibility that the introduction of a new platform may be incompatible with the design of the integrity test, preventing a valid verification. The implementation of the integrity test is designed to fail for any such unrecognized platforms.

4.2 Firmware Security

Multiple integrity checks are performed in the process of generating and running an application using the Module:

- The integrity of the binary ISS HA-ECT FIPS Object Module file is checked before generating the runtime executable application.

When the ISS HA-ECT FIPS Object Module file has been built and validated, a set of HMAC-SHA-256 digests for the FIPS 140-2 validated Module are documented in this Security Policy for each validated platform. When the operator is about to incorporate the ISS HA-ECT FIPS Object Module into the application, the ghash utility is used to compute and display the HMAC-SHA-256 digests corresponding to the Module's code and data. These digests must match the known good digests documented in this Security Policy in order for the Module to be considered FIPS 140-2 validated and the operator to proceed.

- The integrity of the FIPS Module within the application is checked at run-time.

The ghash utility is used by ISS to inject the HMAC-SHA-256 digests within a special read-only data section of the ISS HA-ECT FIPS Shared Object Module. The ISS HA-ECT library's FIPS initialization function, `ect_EnableFIPSMODE()`, will dynamically compute the SHA-256 digests and compare them against these build-time stored values to make sure they match. This run-time check ensures that the ISS HA-ECT library has not been corrupted between application build-time and system run-time.

This chain of integrity checks assures that applications using ISS HA-ECT will use FIPS 140-2 validated cryptography when built using the validated ISS HA-ECT FIPS Shared Object Module.

4.3 Self-Tests

The Module performs a number of power-up and conditional self-tests to ensure proper operation of the Module. Power-up self-tests include cryptographic algorithm known answer tests and integrity tests. Input, output, and cryptographic functions cannot be performed while the Module is in a self-test or error state as the Module is single threaded and will not return to the calling application until the power-up self tests are complete. If the power-up self tests fail, subsequent calls to the Module will fail and thus no further cryptographic operations are possible.

Power-up tests are run automatically when the Module is initialized and do not require any inputs or actions from the module operator. No FIPS-mode cryptographic functionality will be available until after successful execution of all power-up tests. No authentication is required to perform self-tests either automatically or upon demand.

The integrity tests are performed using HMAC-SHA-256 digests calculated over the object code in the ISS HA-ECT FIPS Object Module. The HMAC-SHA-256 key, which is used only for the power-up integrity test, is a key value hard-coded in the module's code. Since this key is used solely for the integrity test, it is not required to be zeroized. The module also stores the integrity hashes, which get integrated into the module upon computation during the library build process. If the computed HMAC-SHA-256 digest matches the stored known digest, then the power-up self-tests consisting of the algorithm specific Sign/Verify and Known Answer tests, are performed. The failure of any power-up self-test or conditional test causes the Module to enter an error state with all cryptographic operations disabled until the Module is reinitialized.

4.3.1 Power-up Self-Tests

Known Answer Tests (KATs) are tests where a cryptographic value is calculated and compared with a stored previously determined answer. The following power-up self-tests are implemented by the Module:

Algorithm	Power-up Self-test
Firmware Integrity Test	Integrity test over all executable code using HMAC-SHA-256 (inclusive of the HMAC and SHA-256 self-test)
AES-GCM-128	Authenticated encryption and decryption KATs with 128-bit key
AES-CCM-128	Encryption and decryption KATs with 128-bit key
SP 800-90A DRBG	SP800-90A section 11.3 health tests for instantiate, generate, and reseed, as well as known answer test
ECDSA nist256p	sign/verify pairwise consistency test with 256 bit key and SHA-256

4.3.2 Conditional Self-Tests

Algorithm	Conditional Test
ECDSA	Pair-wise consistency sign/verify test
DRBG	Continuous random number generator test

4.3.2.1 Sign/Verify Test

A sign/verify test is performed when ECDSA key pairs are generated by signing data with a private key and verifying that signature using the associated public key.

4.3.3 Critical Function Tests

The Module does not implement any critical function tests.

4.3.4 Physical Security

The Module does not claim to enforce any physical security as it is implemented entirely in firmware. Any physical security is enforced by the standard commercial hardware.

4.3.5 Mitigation of Other Attacks

The Module does not mitigate against any specific attacks.

Chapter 5

5 Design Assurance

The Module is managed in accordance with the established configuration management and source version control procedures of the Green Hills Software end user products group. These plans and procedures form part of a comprehensive quality management and improvement system used for all of Green Hills Software's critical products, including operating systems and compilers.

In addition, the ISS HA-ECT Toolkit Module is managed with additional mechanisms to assure the integrity of binary code as delivered and used to create applications.

5.1 Source Code Control

Firmware development functions for ISS HA-ECT software (configuration management, version control, change control, defect tracking) are managed by the ISS group. The source code revisions are maintained in an SVN repository within Green Hills Software's private development team. Individually packaged revisions can be released periodically in electronic archive or portable media form. The integrity of the Module is based on HMAC-SHA-256.

5.2 Application Management of Keys and Critical Security Parameters (CSPs)

Keys and Critical Security Parameters (CSPs)

A Key and Critical Security Parameter (CSP) is information, such as symmetric keys, asymmetric private keys, etc., that must be protected from unauthorized access. Since the Module is accessed via an API from a referencing application, the Module does not manage Keys and CSPs.

The application designer and the end operator share a responsibility to ensure that Keys and CSPs are always protected from unauthorized access. This protection will generally make use of the security features of the host hardware and firmware which is outside of the cryptographic boundary defined for this Module.

Identifying Keys and CSPs

All Keys and CSPs must be created, stored, and destroyed in an approved manner as described by the FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Keys and CSPs are those items of information which must be protected from disclosure, modification, and substitution, such as symmetric keys, asymmetric private keys, etc. Note that the application designer and operator/system administrator/Crypto Officer share a responsibility for protection of Keys and CSPs; the former to include appropriate technical protections and the latter to install and configure the application correctly. Technical protections include checks to require that files storing Keys and CSPs have appropriate permissions (not group writable or world readable, for example). Administrative protections include installation of the runtime firmware (executables and configuration files) in protected locations. End users have a responsibility to refrain from compromising CSPs (as by sending a password in clear text or copying an encryption key to an unprotected location).

The Module includes the following keys and CSPs:

- AES Keys
 - 128-bits, 192-bits, 256-bits
 - CBC, ECB, CTR, GCM, CCM
- ECDSA Private Key
 - P-256 curve
- HMAC-SHA Key
 - SHA-256
- Elliptic-Curve Diffie-Hellman Private Key
 - P-256
- DRBG State
 - AES 128-bits, AES 192-bits, AES 256-bits
 - CTR
 - Seed

The Module includes the following public keys:

- ECDSA Public Key
 - P-256 curve
- EC DH Public Key
 - P-256 curve

Key Generation

The Module API provides cryptographic functions used for asymmetric key generation for ECDSA and for generation of public and private parameters for ECDH. For example, a call to the `IcIECC_GenerateKey ()` API function would be used to generate ECC keys. The control input that drives the invocation of the Module API functions comes from the calling application.

For each of the CSPs used by the module, the keys supplied to the service are externally/user supplied. The module does not generate or establish keys directly.

Storage of Keys and CSPs

The Module only stores the HMAC-SHA-256 key used for the integrity self-test within its binary file. If this key value is modified, the HMAC-SHA-256 value of the Module's binary libect before linking with the application, will be different than the values published in this Security Policy, Appendix A, and will not be considered FIPS-compliant. The Module does not store any other Keys or CSPs in persistent media; while the Module is initialized, all Keys and CSPs reside temporarily in RAM and are destroyed at the end of the session.

Destruction of Keys and CSPs

When no longer needed, Keys and CSPs contained within the application must be deleted by overwriting in a way that will make them unrecoverable (zeroized). The HA-ECT accomplishes this by the user calling algorithm `**_Finish()` API's or when power is removed from the hardware. For ECC keys only, `IcIECC_DestroyKeys()` make keys unrecoverable by zeroization.

Entropy

Because the amount of entropy loaded by the application is dependent on the amount, the minimum number of bits of entropy is considered equal to the key size required by the calling application. The calling application must call the `IcIRand()` with provided entropy of at least 32-bytes (256-bits) to achieve full entropy.

Chapter 6

6 Glossary

Term	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMT	Cryptographic Module Testing
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
CTR	Counter
DH	Diffie-Hellman
ECB	Electronic Codebook
FIPS	Federal Information Processing Standard
FSM	Finite State Machine
GCM	Galois Counter Mode
HA-ECT	High Assurance Embedded Crypto Toolkit (ISS Crypto library)
IV	Initialization Vector
KAT	Known Answer Test
NIST	National Institute of Standards and Technology (USA)
OFB	Output Feedback
OS	Operating System
SHA-256	Secure Hash Algorithm (FIPS 180-4)
HMAC -SHA-256	Keyed-Hash Message Authentication Code (FIPS 198-1)

Chapter 7

7 References

- FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001, National Institute of Standards and Technology
- FIPS PUB 197, Advanced Encryption Standard (AES), 26 November 2001, National Institute of Standards and Technology
- FIPS 186-4, The Digital Signature Standard, July 2013, National Institute of Standards and Technology
- The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) , 15 November 2002, National Institute of Standards and Technology
- Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, Initial Release: March 28, 2003, Last Update: December 23, 2010, National Institute of Standards and Technology
- FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008, National Institute of Standards and Technology
- FIPS 180-4, Secure Hash Standard (SHS), October 2008, National Institute of Standards and Technology
- Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, January 04, 2011 (draft), National Institute of Standards and Technology
- Green Hills Software ISS HA-ECT API Guide

Appendix A – Installation, Validation and Initialization

These instructions assume the following:

- The reader has the basic knowledge of how to unpack the Module’s binary distribution.
- Target environment is as specified in section 2 of this policy

A.1 Module Validation

The Green Hills Software, ISS HA-ECT FIPS Object Module v3.0.3 consists of the FIPS Object Module generated from the specific source files found in the specific Green Hills distribution, *ISS_HA_ECT.tar.gz*. The set of files specified in this tar file constitutes the complete set of source files of this Module. There shall be no additions, deletions, or alterations of this set as used during Module build.

IAR v7.40.1.8472
Target: firmware

After receiving the libect library from Green Hills Software, generate and print the SHA-256 digest for the installed Module using sha256sum. The following command can be used to display the digests of the Module:

```
sha256sum libect.a
```

The Crypto Officer should compare this digest with the below published value for your applicable platform to confirm that the Module is authentic and unmodified.

SHA-256 digest:

libect.a SHA-256 Hash: 87fe7c0e63b9f477d6d842da583de0a941391ca7060758477e10cdc4a4e796dd

A.2 Installing and Protecting the ISS HA-ECT FIPS Object Module

The Module should be installed within the operator’s configuration management system by the Crypto officer such that it is protected from unauthorized modification. In particular, operators using the object Module to build an application should only have read access to the object Module.

A.3 Linking the Runtime Executable Application

Once the Crypto Officer has confirmed the digests match, ensuring the correct/valid crypto library is being used, the library can be linked into the application by adding libect.lib to each corresponding program. After the library is linked into the application, the user supplied program, ghash, must be run on the application. Ghash computes the HMAC-SHA-256 digests along with the starting addresses of the .ecttext and .ectrodata sections and injects the information into the .ecthash section. The application is now considered Module-enabled. The Crypto officer should install the Module-enabled application in a location protected by the host operating system security features. These protections should allow write access only to Crypto Officers and read access only to authorized users. Note that applications code interfacing with the ISS HA-ECT FIPS Object Module are outside of the cryptographic boundary, although the entire application must be write-protected since the Module is now linked with the application.

Failure to embed the digest in the executable object will prevent initialization of FIPS mode. At runtime, the ect_EnableFIPSMode() function compares the HMAC-SHA-256 digests from the module's binary with the digests generated from the Module-enabled application. These digests are the final link in the chain of validation from the original Module binary to the runtime executable application file.