Geotab Inc.

Geotab Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

GEOTAB
management by measurement

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 5
2 Cryptographic Module Specification 5
2.1 Description 5
System description 6
Module Boundary 6
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 9
Non-Approved security functions 10
2.6 Security Function Implementations 10
2.7 Algorithm Specific Information 11
2.8 RBG and Entropy 11
RBG entropy sources 11
2.9 Key Generation 12
2.10 Key Establishment 12
2.11 Industry Protocols 12
3 Cryptographic Module Interfaces 12
3.1 Ports and Interfaces 12
4 Roles, Services, and Authentication 12
4.1 Authentication Methods 13
4.2 Roles 13
4.3 Approved Services 13
4.4 Non-Approved Services 15
4.5 External Software/Firmware Loaded 15
5 Software/Firmware Security 15
5.1 Integrity Techniques 15
5.2 Initiate on Demand 16
6 Operational Environment 16
6.1 Operational Environment Type and Requirements 16

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

7 Physical Security....16
8 Non-Invasive Security....16
9 Sensitive Security Parameters Management....17
9.1 Storage Areas....17
9.2 SSP Input-Output Methods....17
9.3 SSP Zeroization Methods....17
9.4 SSPs....18
10 Self-Tests....20
10.1 Pre-Operational Self-Tests....20
10.2 Conditional Self-Tests....20
10.3 Periodic Self-Test Information....22
10.4 Error States....23
11 Life-Cycle Assurance....23
11.1 Installation, Initialization, and Startup Procedures....23
Installation....23
Initialization....23
Startup Procedure....23
11.2 Administrator Guidance....23
11.3 Non-Administrator Guidance....23
11.4 End of Life....23
11.5 Additional Information....24
12 Mitigation of Other Attacks....24

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 8
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 8
Table 4: Modes List and Description 9
Table 5: Approved Algorithms 10
Table 6: Vendor-Affirmed Algorithms 10
Table 7: Security Function Implementations 11
Table 8: Entropy Certificates 11
Table 9: Entropy Sources 12
Table 10: Ports and Interfaces 12
Table 11: Roles 13
Table 12: Approved Services 15
Table 13: Storage Areas 17
Table 14: SSP Input-Output Methods 17
Table 15: SSP Zeroization Methods 17
Table 16: SSP Table 1 18
Table 17: SSP Table 2 20
Table 18: Pre-Operational Self-Tests 20
Table 19: Conditional Self-Tests 22
Table 20: Pre-Operational Periodic Information 22
Table 21: Conditional Periodic Information 22
Table 22: Error States 23

List of Figures

Figure 1. Cryptographic Boundary 7

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

1 General

1.1 Overview

This document is the non-proprietary security policy for the Geotab Cryptographic Module from Geotab Inc. This Security Policy describes how the Geotab Cryptographic Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3 for security level 1.

1.2 Security Levels

The following table lists the level of validation for each area in FIPS-140-3

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

Reference	Description
140-3 IG	FIPS 140-3 Implementation Guidance

2 Cryptographic Module Specification

2.1 Description

The Geotab Cryptographic Module, hereafter referred to as the module, is classified as **Level 1 Firmware Module** as per FIPS-140-3 guidelines operating within a limited operational environment. The module operates with a single-chip standalone module embodiment. The cryptographic boundary is the module's binary i.e. fipslib.bin. The module is bundled with the firmware image used by the physical microcontrollers. The module performs no communication other than with the calling application via well-defined APIs that invoke the Module.

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

System description

The system described by this security policy is a single-chip firmware module, running in a limited operational environment which loads an application and appends the validated module binary, that requires a power-on reset to install. The operating environment does not have an operating system and contains a single CPU with one core. The environment is single threaded and parallel execution is not possible. Program instructions of the module and volatile SSPs are stored within the cryptographic boundary. The module does not provide non-volatile key storage. Keys are provided externally by the application layer and are not stored by the module in non-volatile memory.
Module Type: Firmware

Module Embodiment: Single Chip

Module Characteristics:

Module Boundary

The following block diagram details modules' Tested Operational Environment’s Physical Perimeter and Cryptographic boundaries.

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

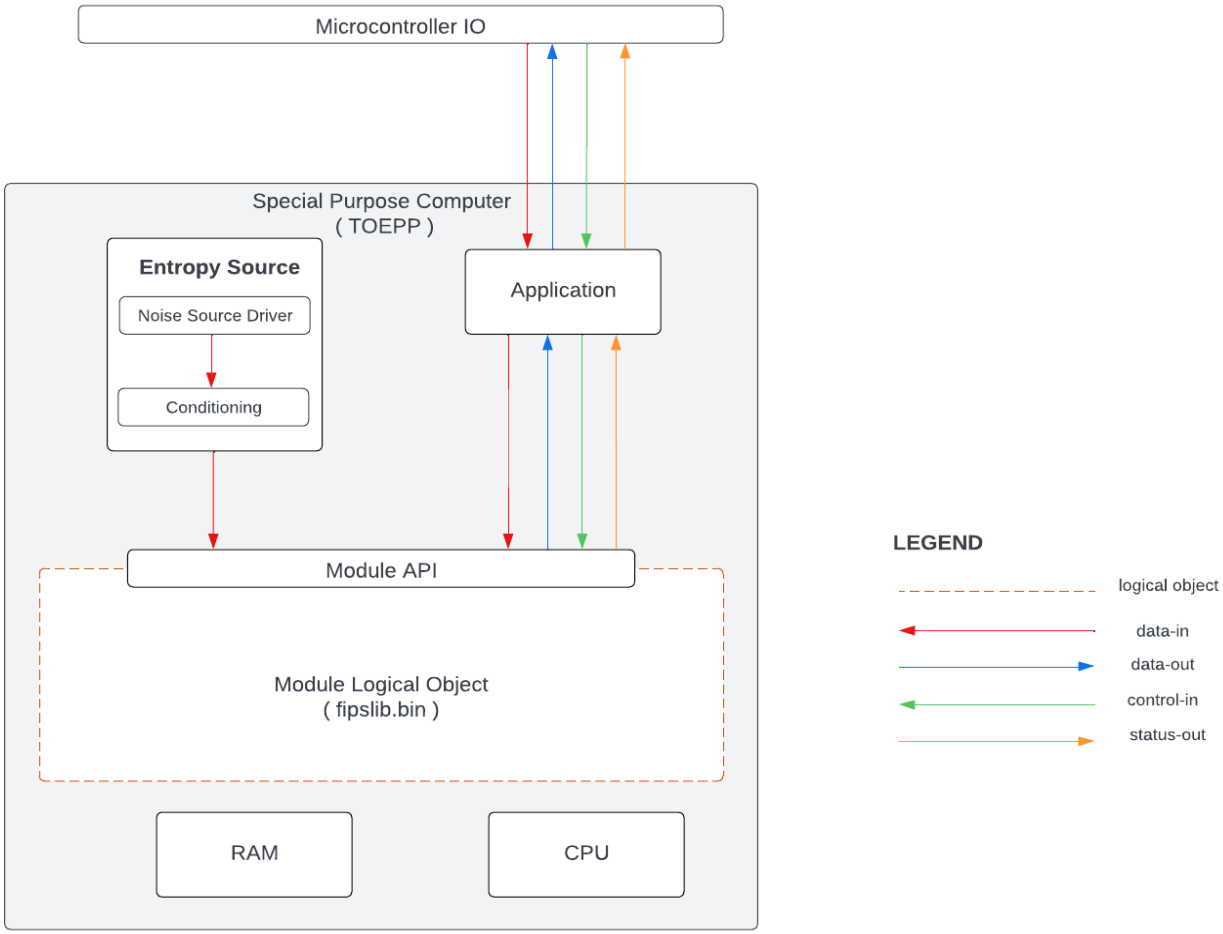


Figure 1. Cryptographic Boundary

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Tested Operational Environment's Physical Perimeter (TOEPP):

Per figure 1, the Tested Operational Environment's physical perimeter is the S32K Core Telematics Board and STM32H7 Core Telematics Board that the module operates on.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fipslib.bin	2.0	Compiled for ARM Cortex M4F on NXP S32K14X (Armv7E-M)	Yes
fipslib.bin	2.0	Compiled for ARM Cortex M7 on STM32H7 (Armv7E-M)	Yes

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

The product has been tested and is intended to operate on the following Geotab Operating Environments. There are no Vendor affirmed operational environments.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Apache Nuttx	S32K Core Telematics Board	NXP S32K14X (Armv7E-M)	No		2.0
Apache Nuttx	STM32H7 Core Telematics Board	STM32H7 (Armv7E-M)	No		2.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

2.3 Excluded Components

There are no excluded components

2.4 Modes of Operation

Modes List and Description:

The following are the modes of operation and their description mentioned in the Table below.

Mode Name	Description	Types of Services	Status Indicator
Approved Mode of Operation	The mode of operation in which the module is operating correctly	Approved	Successful completion of service

Table 4: Modes List and Description

The module does not support any operation in a degraded mode.
In the approved mode of operation, the *"Get Version"* service will return an integer value corresponding to the module revision which is 2.0.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4203	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
HMAC DRBG	A4203	Prediction Resistance - No Supports Reseed - No Mode - SHA2-256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0 Returned Bits - 256	SP 800-90A Rev. 1
HMAC-SHA2-256	A4203	MAC - MAC: 256 Key Length - Key Length: 256	FIPS 198-1
RSA SigVer (FIPS186-5)	A4203	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048 Signature Type - pkcs1v1.5	FIPS 186-5

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Algorithm	CAVP Cert	Properties	Reference
		Fixed Public Exponent - 010001 Public Exponent Mode - fixed	
SHA2-256	A4203	Message Length - Message Length: 0-51200 Increment 8 Function - SHA2	FIPS 180-4

Table 5: Approved Algorithms

Note: Only the algorithms specified in the table above are supported by the module in approved mode of operation

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric	N/A	SP 800-133r2 Sections 4, Example 1

Table 6: Vendor-Affirmed Algorithms

Non-Approved security functions

The module does not support any of the following:
“Non-Approved, Allowed Algorithms”,
"Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed",
“Non-Approved, Not Allowed Algorithms”.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES-CBC	BC-UnAuth	Used for Authentication & encryption		AES-CBC: (A4203)

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Name	Type	Description	Properties	Algorithms
CKG	CKG	Symmetric key generation using unmodified HMAC_DRBG output		HMAC DRBG: (A4203) HMAC-SHA2-256: (A4203) SHA2-256: (A4203)
DRBG	DRBG	Deriving Entropy		HMAC DRBG: (A4203) HMAC-SHA2-256: (A4203) SHA2-256: (A4203)
HMAC	MAC	Integrity Check		HMAC-SHA2-256: (A4203) SHA2-256: (A4203)
SHA	SHA	Hash Function		SHA2-256: (A4203)
SigVer	DigSig-SigVer	Signature Verification		RSA SigVer (FIPS186-5): (A4203) SHA2-256: (A4203)

Table 7: Security Function Implementations

The Security Function implementations are mentioned in the table above.

2.7 Algorithm Specific Information

No additional information.

2.8 RBG and Entropy

RBG entropy sources

The entropy source resides outside the module's cryptographic boundary but within the module’s physical perimeter.

Cert Number	Vendor Name
E86	Geotab Inc.

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Accelerometer Based Entropy Source	Physical	NXP S32K14X (Armv7E-M), STMicroelectronics STM32H7 (Armv7E-M)	256 bits	256 bits	A4203 (SHA2-256)

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Table 9: Entropy Sources

The DRBG requests 512-bits from the entropy source which outputs full entropy.

2.9 Key Generation

The module generates 256-bit AES keys and HMAC keys per SP 800-133r2 Sections 4 and 6.1 as the unmodified output of the approved HMAC_DRBG (A4203), which supports a security strength of 256 bits. The keys are output to the calling application through the Random Bit Generation and Symmetric Key Generation service (IG D.H Additional Comment 2).

2.10 Key Establishment

This module does not support any Key Agreement Schemes.

2.11 Industry Protocols

None

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The physical ports of the module are the same as the special purpose single chip microcontroller system on which it is executing. The logical interface is an application programming interface (API), the mapping of logical interface type is explained below.

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API entry point data input parameters
N/A	Data Output	API entry point data output parameters
N/A	Control Input	API entry point and corresponding parameters
N/A	Status Output	API entry point return values
N/A	Power	N/A

Table 10: Ports and Interfaces

Since the module boundary is firmware, control of the physical ports is outside the module scope. When the module is in self-test state, error state or zeroization state, all output on the logical data output interface is prohibited. In error state module will only return error value (no data output is returned).

4 Roles, Services, and Authentication

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

4.1 Authentication Methods

N/A for this module.

The module does not support operator authentication.

4.2 Roles

The module supports following role:

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO)	Role	Crypto Officer	None

Table 11: Roles

The module supports the Crypto Officer (CO) role and does not support multiple concurrent roles or any maintenance or bypass capability. The CO role is implicitly assumed by the application accessing services implemented by the module.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize Module	Initializes the module and runs the designated self tests.	Successful completion of service (Status = 0)	Module Integrity Value	Status	None	Crypto Officer (CO)
RSA Signature	Generate or verify digital signatures	Successful completion of service (Status = 0)	Sign: Digital Signature - Generation Key Verify: Digital Signature - Verification Key,	Sign: Status, signature value. Verify: status	SigVer	Crypto Officer (CO) - RSA Signature - Verification Key: W,E
Get State	Provide Module state	Module state is provided.	API command	Module State	None	Crypto Officer (CO)
Get Version	Provides Module Version	Module Version is provided.	API command	Module Version	None	Crypto Officer (CO)

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Keyed Hash	Generate or verify message integrity	Successful completion of service (Status = 0)	Message, Keyed Hash Key	Status, Hash Value	HMAC	Crypto Officer (CO) - Keyed Hash Key: W,E
Message Digest	Generate a message digest	Successful completion of service (Status = 0)	Message	Status, Hash Value	SHA	Crypto Officer (CO)
Random Bit Generation and Symmetric Key Generation	Generate random bits using the HMAC_DRBG. The output is used directly as a 256-bit AES or HMAC symmetric key (CKG), or as random bits for other uses, such as IVs	Successful completion of service (Status = 0)	Number of bits to generate, Entropy Seed	Status, randomly generated bits.	DRBG CKG	Crypto Officer (CO) - Entropy Input String: G,E - Entropy Seed: G,E - DRBG Hash Key: G,E - Secret V: G,E - Symmetric Cipher Key - CBC: G,R - Keyed Hash Key: G,R
Symmetric Ciphers	Encrypt or Decrypt data with AES including CBC modes.	Successful completion of service (Status = 0)	Symmetric Cipher Key	Status, Plaintext or Ciphertext data	AES-CBC	Crypto Officer (CO) - Symmetric Cipher Key - CBC: W,E
Zeroize	Zeroize all SSPs by power-cycling the module.	Module re-initializes and successfull	None (power removal)	Status	None	Crypto Officer (CO) - Entropy

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Removing power clears volatile memory, setting all SSP instances to zero and rendering them non-retrievable.	y completes the pre-operational self-tests on next power-up				Input String: Z - Entropy Seed: Z - Keyed Hash Key: Z - Symmetric Cipher Key - CBC: Z - DRBG Hash Key: Z - Secret V: Z - RSA Signature - Verification Key: Z

Table 12: Approved Services

The indicator field of the above table specifies the “successful completion of service” means Services return success status; non-zero value or the approved security function finishes successfully.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

N/A for this module.

5 Software/Firmware Security

5.1 Integrity Techniques

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

The firmware module is in the form of a compiled binary called fipslib.bin which is a subset of the overall firmware binary. (geotab.bin = businesslogic.bin + fipslib.bin).

After a module is powered on, the module's integrity check using HMAC-SHA2-256 (A4203) is performed during module instantiation. If the Integrity check fails, it will cause the module to enter an error state. All the temporary values generated during the integrity check are zeroized upon completion of the operation.

Additionally, the module performs listed self-tests and if successful the module will enter the Operational State.

5.2 Initiate on Demand

The operator is able to initiate the integrity test on demand by re-initializing the module or by power-cycling the host platform. Upon initialization the module performs an integrity test of the module on itself using HMAC-SHA2-256 (A4203). If the Integrity check fails, it will cause the module to enter an error state.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The Module tested operating environments are listed below. The module implements limited operating environment. The module functions entirely within the Operating environment provided space for the calling application.

- NXP S32K148 with ARM CORTEX M4F series processor
- ST STM32H7 with the ARM CORTEX M7 Series Processor

7 Physical Security

The module is a single-chip cryptographic module and composed of production grade components. The module obtains its physical security from a single chip with standard passivation coating which protects against any environmental or physical damage. As the module consists of production grade components with standard passivation it satisfies the security requirements of Security Level 1.

8 Non-Invasive Security

This cryptographic module does not claim any non-Invasive security features.

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Volatile Memory area where all SSPs are stored	Dynamic

Table 13: Storage Areas

All Sensitive Security Parameters (SSPs) are stored in volatile memory in plaintext format.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API Interface - Input	Volatile Memory outside the module boundary	RAM	Plaintext	Manual	Electronic	
API Interface - Output	RAM	Volatile Memory outside the module boundary	Plaintext	Manual	Electronic	

Table 14: SSP Input-Output Methods

All SSPs Input Output methods are specified in the table above.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroize service	Power Cycle - Sets the SSPs to 0 when the module is powered off.	Power loss to clear SSP values stored in volatile memory	Unplug the device

Table 15: SSP Zeroization Methods

All temporary SSP values in volatile memory used are zeroized. The zeroization consists of writing zeros to the memory location used by the SSP. The zeroization service for the SSP in volatile memory consists of powering off the module, which sets all instances of SSPs to 0 value and making it non-retrievable.

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

9.4 SSPs

The module receives all SSPs through API calls to the module. With the exception of symmetric keys generated by the Random Bit Generation and Symmetric Key Generation service and the DRBG internal state, all SSPs are provided externally to the module and handled by the application using the module.

The module supports the following SSP's listed below

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Symmetric Cipher Key - CBC	AES Key used for encryption and decryption operations for AES CBC mode	256-bits - 256-bits	Symmetric key - CSP	CKG		AES-CBC
Keyed Hash Key	Key for keyed hash service.	256 bits - 256 bits	Symmetric Key - CSP	CKG		HMAC
RSA Signature - Verification Key	RSA Algorithm key for signature verification	2048 bits - 112 bits	Asymmetric Key - CSP			SigVer
Entropy Input String	Entropy input string from external entropy source.	512 bits - 512 bits	Entropy - CSP			DRBG CKG
Entropy Seed	Seed entropy taken from Entropy Input String	256 bits - 256 bits	Entropy - CSP			DRBG CKG
DRBG Hash Key	Hash DRBG Internal state secret Key	256 bits - 256 bits	Entropy - CSP	DRBG CKG		DRBG CKG
Secret V	Hash DRBG Internal state secret V	256 bits - 256 bits	Entropy - CSP	DRBG CKG		DRBG CKG

Table 16: SSP Table 1

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Symmetric Cipher Key - CBC	API Interface - Input API Interface - Output	RAM:Plaintext	Power-Cycle	Zeroize service	DRBG Hash Key:Generated from Secret V:Generated from
Keyed Hash Key	API Interface - Input API Interface - Output	RAM:Plaintext	Power-Cycle	Zeroize service	DRBG Hash Key:Generated from Secret V:Generated from
RSA Signature - Verification Key	API Interface - Input	RAM:Plaintext	Power-Cycle	Zeroize service	
Entropy Input String	API Interface - Input	RAM:Plaintext	Power-Cycle	Zeroize service	Entropy Seed:Generates
Entropy Seed		RAM:Plaintext	Power-Cycle	Zeroize service	Entropy Input String:Generated From Secret V:Generates DRBG Hash Key:Generates
DRBG Hash Key		RAM:Plaintext	Power-Cycle	Zeroize service	Entropy Seed:Generated From Secret V:Used With Symmetric Cipher Key - CBC:Generates Keyed Hash Key:Generates
Secret V		RAM:Plaintext	Power-Cycle	Zeroize service	Entropy Seed:Generated From DRBG Hash Key:Used With Symmetric Cipher Key - CBC:Generates Keyed Hash Key:Generates

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Table 17: SSP Table 2

10 Self-Tests

If any self-test fails, the module enters an error state. To attempt to clear the error, re-initialize the module. A power cycle is required in order to run power on self-tests on demand.

10.1 Pre-Operational Self-Tests

The Pre-operational self-test is listed in the table below. The algorithm used in the integrity test i.e. HMAC SHA2-256 is tested before it is used in the integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A4203)	256-bits key length	KAT	SW/FW Integrity	Return success	Integrity test performed on the module image. Integrity verified using HMAC SHA-256.

Table 18: Pre-Operational Self-Tests

The module does not support bypass.
The module does not implement any pre-operational critical function tests.

10.2 Conditional Self-Tests

All the Conditional Cryptographic Algorithm Tests (CAST) are listed here in the table below. All CASTs must pass before the module can operate.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Adaptive Proportion Test	Window size: 1024, Cutoff: 652	Fault Detection	CAST	Returns success	Checks the proportion of ones and zeros in consecutive DRBG output blocks.	Entropy Collection
AES-CBC Decrypt (A4203)	Key length - 256 bits	KAT	CAST	Returns success	Decryption	Power-on
AES-CBC Encrypt (A4203)	Key length - 256 bits	KAT	CAST	Returns success	Encryption	Power-on

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A4203)	SHA-256, 256-bit security strength	KAT	CAST	Returns success	Random Number Generator	Power-on
HMAC DRBG Continuous Test	16 bytes comparison length	Continuous test	CAST	Returns success	Confirms that the DRBG output is not stuck when new seed is requested	Service Invocation
HMAC DRBG Test Generate	256-bits output length	KAT	CAST	Returns success	Confirms DRBG generation	Power-on
HMAC DRBG Test Instantiate	SHA-256, 256-bit entropy input, 128-bit nonce	KAT	CAST	Returns success	confirm the DRBG instantiation	Power-on
HMAC DRBG Test Un-instantiate	Zeroization verification of DRBG context	KAT	CAST	Returns success	error handling and the internal state has been zeroized	Power-on
HMAC-SHA2-256 (A4203)	256 bits	KAT	CAST	Returns success	HMAC	Power-on
Repetition Count Test	Cutoff: 26 consecutive bits	Fault Detection	CAST	Returns success	Checks for repeated output blocks from the DRBG.	Entropy Collection
RSA SigVer (FIPS186-5) (A4203)	Key length-2048 bits	KAT	CAST	Returns success	Signature Verification	Power-on
SP 800-90B Health Tests	1024 minimum samples, Continuous: 128-bit (16-byte) conditioned entropy comparison	Fault Detection	CAST	Returns success	Confirms working of conditioned entropy source	Power-on
HMAC DRBG Test Reseed	SHA-256, 256-bit security	KAT	CAST	Returns success	Confirms the DRBG reseed function	Power-on

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	strength, additional entropy input					

Table 19: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A4203)	KAT	SW/FW Integrity	On Demand	Power cycle

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Adaptive Proportion Test	Fault Detection	CAST	On Demand	Power cycle
AES-CBC Decrypt (A4203)	KAT	CAST	On Demand	Power cycle
AES-CBC Encrypt (A4203)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A4203)	KAT	CAST	On Demand	Power cycle
HMAC DRBG Continuous Test	Continuous test	CAST	On Demand	Power cycle
HMAC DRBG Test Generate	KAT	CAST	On Demand	Power cycle
HMAC DRBG Test Instantiate	KAT	CAST	On Demand	Power cycle
HMAC DRBG Test Un-instantiate	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A4203)	KAT	CAST	On Demand	Power cycle
Repetition Count Test	Fault Detection	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-5) (A4203)	KAT	CAST	On Demand	Power cycle
SP 800-90B Health Tests	Fault Detection	CAST	On Demand	Power cycle
HMAC DRBG Test Reseed	KAT	CAST	On Demand	Power cycle

Table 21: Conditional Periodic Information

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

The module does not support periodic self-testing.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Module in Error State	All outputs are inhibited once it transitions to the error state	If Integrity test or KAT fails, enter error state	Power-Cycle	Initialize Module service returns a non-zero value.

Table 22: Error States

Integrity tests and self-tests can fail and result in error status as mentioned in the table above.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Installation
The Module is already installed as part of the main firmware for the device. The device is already installed with the main firmware which includes the cryptographic module.

Initialization
The Module is initialized by calling the Initialize Module service. The initialization procedure shall be invoked by the CO Role. The CO role has responsibility to ensure that the 'Initialize Module' service returns a successful indicator before the usage of the module begins.

Startup Procedure
The device is powered on. After entering into the initialization state an integrity check is performed. Then the Module performs self-tests. Upon successful completion of the self-tests, the module enters in Operational state.

11.2 Administrator Guidance

Please contact *embeddedsecurity@geotab.com* for Administrator guidance.

11.3 Non-Administrator Guidance

The module supports the CO role and does not support non-administrators or non-administrative roles.

11.4 End of Life

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.

The procedure for secure sanitization of the module is to power it off, which is the action of zeroization of the SSPs. The sanitization via power-off, results in removal of SSPs from the module.

11.5 Additional Information

Configuration Management

The code repositories are managed through Git-based configuration management and version control systems. Production grade C/C++ (gcc) compilers and assemblers are used for the development.

Platform	Hardware	Compiler	Configuration
N/A	NXP S32K148	gcc-arm-none-eabi	-fno-builtin -Wall -Werror -Wstrict-prototypes -Wshadow -Wundef -g -mcpu=cortex-m4 -mthumb -mfloat-abi=hard -mfpu=fpv4-sp-d16 -O1-Wl,--fatal-warnings
N/A	ST STM32H7	arm-none-eabi-gcc	-fno-builtin -Wall -Werror -Wstrict-prototypes -Wshadow -Wundef -g -mcpu=cortex-m7 -mthumb -mfloat-abi=hard -O1-Wl,--fatal-warnings
Platform	Hardware	Compiler	Configuration

Table : Compilers

Platform	Hardware	Linker	Configuration
N/A	NXP S32K148	gcc-arm-none-eabi	n/a
N/A	ST STM32H7	arm-none-eabi-gcc	n/a

Table : Linkers

The module does not claim any authentication functionality.

12 Mitigation of Other Attacks

The module does not claim to mitigate any additional attacks.

Copyright © Geotab Inc. 2023 - All Rights Reserved | www.geotab.com
® denotes a trademark of Geotab Inc., which may be registered in certain countries
This document may freely be reproduced and distributed in its entirety.