FESCARO Cryptographic Module

FAST C-LIB v1.0.0

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.1.8

Last Update: 07/22/2022

Revision History

	Date	Author	Description
1.1.7	05/28/2021	Fescaro Co.Ltd.	Initial Release
1.1.8	07/22/2022	Fescaro Co.Ltd.	CAVP Cert #A2722 added, Appendix A: Security Rules are modified

Index

1. Introduction

1.1 Purpose

This document is a non-proprietary FIPS 140-2 Security Policy for FAST C-LIB from FESCARO Co.Ltd. This Security Policy describes how the FAST C-LIB meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2 for a Security Level 1 multi-chip standalone software module.

1.2 Copyright

2. Cryptographic Module Specification

2.1 Module Overview

The FAST C-LIB is software cryptographic library embedded in vehicle ECUs. The FAST C-LIB is used to meet OEM's automotive security requirements. For example, the FAST C-LIB is used to implement secure In-Vehicle communication and secure V2X communication.

2.2 Module Validation Level

The following table shows the overview of the security level for each the eleven requirements sections of the validation.

FIPS 140-2 Security Requirements Sections		Security 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	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
Overall Level		1

Table 1 Module Validation Level

2.3 Module Specification

The FAST C-LIB is a software cryptographic module with a multi-chip standalone embodiment. The overall FIPS 140-2 security level of the module is 1. The software version of the module is 1.0.0.

The FAST C-LIB was tested and found to be FIPS 140-2 compliant on the following platform:

Evaluation Board	GPC (MCU)	Processor (CPU)	Operating System
ShieldBuddy TC275	Infineon AURIX TC275TP (SAK-TC275TP-64F200N DC)	ARM Cortex M3 (HSM Core)	OSEK/VDX OS 2.2.3

Table 2 Tested Platform

2.3.1 Physical Cryptographic Boundary

The FAST C-LIB is a software cryptographic module, so there are no physical protection mechanisms implemented. Therefore, the module must rely on the physical characteristics of the GPC.

The GPC consists of three host cores (TriCore) and one HSM Core (ARM Cortex M3) and peripherals. The FAST C-LIB software runs in HSM domain (HSM Core and HSM peripherals). All CSPs for the FAST C-LIB are stored in HSM Flash and HSM SRAM. According to physical security characteristics of the MCU, HSM domain is not accessible from the any other domain such as host cores.

NOTE #1: The FAST C-LIB does not use the AES128 HW module in Figure 1 when performing AES encryption/decryption and CMAC generation/verification. These operations are performed in their entirety inside of the FAST C-LIB Software boundary depicted in Figure 2.

NOTE #2: The FAST C-LIB use output of TRNG HW module as DRBG entropy input.

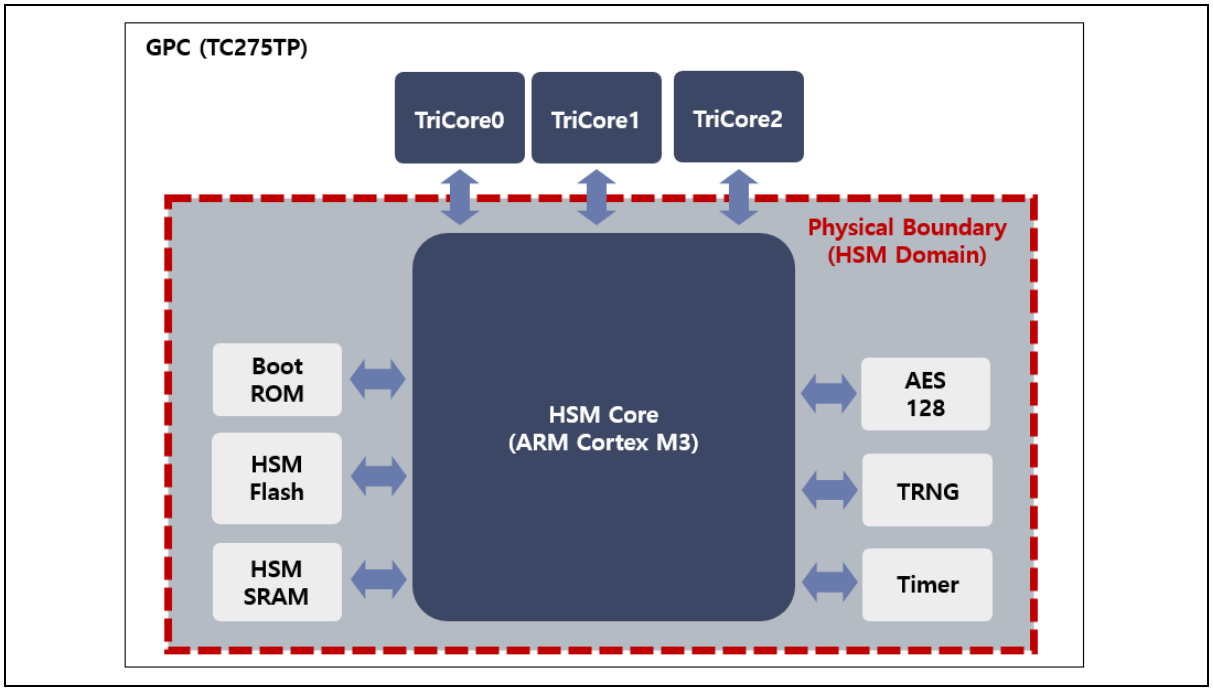

Figure 1 Hardware Block Diagram

2.3.2 Logical Cryptographic Boundary

The software block diagram below shows the logical boundary of the FAST C-LIB and its interfaces overview with the User Application.

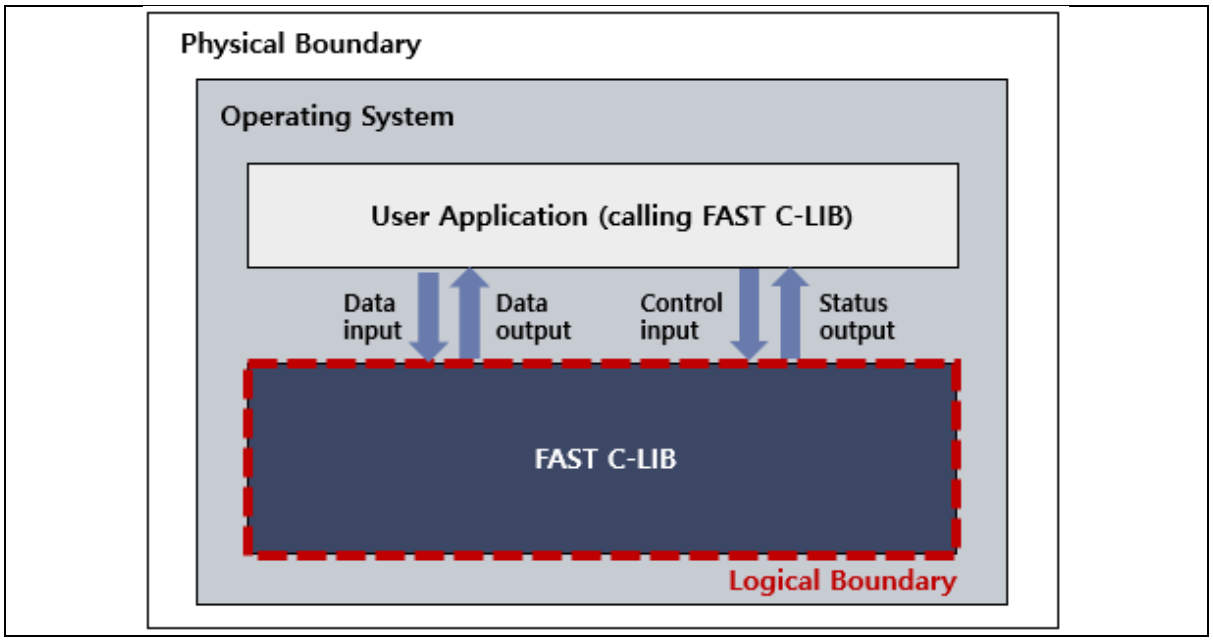

Figure 2 Software Block Diagram

2.3.3 Operation Mode Description

The FAST C-LIB supports FIPS Approved mode (i.e. Approved mode of operation) only. After successful completion of power-up self-tests, the module enters FIPS Approved mode implicitly. Approved cryptographic algorithms are listed in below table. Cert # column is algorithm validation numbers that obtained from NIST based on the CAVP testing of the cryptographic algorithm implementations on the Table 2: Tested Platform.

NOTE #1: The FAST C-LIB does not support RSA Encryption/Decryption function and DSA Domain Parameter Generation/Verification function in FIPS Approved mode. This is latent functionality tested during CAVP Cert. #C1842, that is not exposed by the module to the consuming application.

NOTE #2: DSA key pair is used for DH Key Agreement usage only. DSA is not exposed as an API and only tested as a pre-requisite for KAS FFC DH.

NOTE #3: In case of KDF, there is no CAVP Cert #, but the vendor has affirmed this algorithm.

NOTE #4: The consuming application that have a Crypto Officer role must call the ShowStatus API to check if the module is in FIPS approved mode.

NOTE #5: FAST C-LIB directly uses the output (U) from approved HMAC-DRBG to generate symmetric and asymmetric key pairs.

NOTE #6: The HASH-DRBG is not used by the module for Key Generation; this DRBG only supports random number generation

NOTE #7: The AES GCM IV is generated entirely randomly by the SP 800-90A DRBG according to Technique #2 of IG A.5. The IV length is 96 bits.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths or Moduli	Use
C1842	SHS	FIPS 180-4	SHA-256, SHA-512	N/A	Message Digest
C1842	RSA SigGen	FIPS 186-4	SHA-256 PKCS 1.5, PKCSPSS	2048	Digital Signature Generation
C1842	RSA SigVer	FIPS 186-4	SHA-256 PKCS 1.5, PKCSPSS	2048	Digital Signature Verification
C1842	RSA Decryption	SP 800-56B	N/A	2048	Not used
C1842	RSA KeyGen	FIPS 186-4	N/A	2048	RSA Key-pair Generation
C1842	AES	FIPS 197	ECB, CBC	128	Data Encryption/Decryption
C1842	AES	FIPS 197	CTR	128	Data Encryption
C1842	GCM	SP 800-38D	AES-GCM	128	Data Encryption/Decryption
C1842	CMAC	SP 800-38B	N/A	128	Message Authentication Code Generation/Verification
Vendor Affirmation	CKG	SP 800-133r1	N/A	N/A	FAST C-LIB directly uses the output (U) from approved HMAC-DRBG to generate symmetric and asymmetric key pairs.
C1842	HMAC	FIPS 198-1	SHA-256, SHA-512	256, 512	Message Authentication Code Generation/Verification
C1842	DRBG	SP 800-90A	HMAC-SHA-256, HMAC-SHA-512	N/A	Deterministic Random Bit Generation
C1842	DRBG	SP 800-90A	HASH-SHA-256, HASH-SHA-512	N/A	Deterministic Random Bit Generation
C1842	DSA	FIPS 186-4	N/A	(2048,256)	DSA Key-pair

	KeyGen				Generation
C1842	DSA PQGGen	FIPS 186-4	SHA-256	(2048,256)	DSA PQG Generation
C1842	DSA PQGVer	FIPS 186-4	SHA-256	(2048,256)	DSA PQG Verification
A2722	KAS	SP 800-56Ar3	C(2e, 0s, FFC DH)	2048	Key Agreement

Table 3 FIPS Approved Algorithm Lists

3. Cryptographic Module Ports and Interfaces

As a software-only module, the FAST C-LIB does not have physical ports. For the purpose of FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which it runs. The following table summarizes the physical interfaces of ShieldBuddy TC275.

Physical Interface/Port	FAST C-LIB Relevance
Physical power connector	Apply power to the module
Physical DAP3 connector	Control and Data Input for the module
Physical micro USB connector	N/A

Table 4 Physical Interfaces available in the tested platform

When the module is performing self-tests, or the module is in error state (i.e. Fatal or Simple Error state), all output on the logical data output is inhibited. The module in error state (i.e. Fatal or Simple Error state) returns only an error value, and no data output is returned.

The logical interfaces are various application programming interfaces (API). The logical interfaces of the module expose services that applications can call. The following table summarizes the four logical interfaces:

NOTE: The FAST C-LIB does not output any CSPs through logical interface.

Logical Interface	Description
Data Input	API input parameters
Data Output	API output parameters
Control Input	API function calls
Status Output	API return values, API output parameters for status and error

Table 5 Ports and Interfaces

4. Roles, Services, and Authentication

4.1 Roles

The FAST C-LIB supports the User and Crypto Officer (CO) roles. The two roles are explicitly assumed depending on the config_customer.h setting. Depending on the setting, the module will make the proper services available to the operator as per Table 6. The module does not support for maintenance role and multiple concurrent operators.

NOTE: Refer to 4.2 Services for more information on the services available for each role.

- User: In the field after vehicle production / Limited service available only
- Crypto Officer (CO): In the field before vehicle production / All service available

4.2 Services

The FAST C-LIB provides the following services:

NOTE: Refer to Table 3: FIPS Approved Algorithm Lists for more information about CAVP Cert #.

Role	Service	Algorithm	Cryptographic Keys, CSPs and Public Keys	Type(s) of Access
User, CO	Hash Generation (SHA-256, SHA-512)	SHS	N/A	N/A
User, CO	RSA Signatures Generation (SigGenPKCS1.5 with SHA-256, SigGenPSS with SHA-256)	RSA SigGen	RSA private key with 2048 bits modulus size	Read
User, CO	RSA Signatures Verification (SigVerPKCS1.5 with SHA-256, SigVerPSS with SHA-256)	RSA SigVer	RSA public key with 2048 bits modulus size	Read
User, CO	AES Encryption and Decryption (ECB, CBC and CTR modes)	AES	128 bits AES key	Read
User, CO	GCM Encryption and Decryption	GCM	128 bits AES key	Read
User, CO	Message Authentication	CMAC	128 bits AES key,	Read
		HMAC (SHA-256, SHA-512)	256/512 bits HMAC key	Read
User, CO	Random Number Generation (HMAC_DRBG with/without PR, Hash_DRBG with/without PR)	HMAC_DRBG (HMAC-SHA-256, HMAC-SHA-	32 bits DRBG Entropy input string, 256/512 bits V, 256/512 bits Key	Read, Write, Read

		512)		
		HASH_DRBG (SHA-256, SHA-512)	32 bits DRBG Entropy input string, 440/888 bits V, 440/888 bits C	Read, Write, Write
User, CO	RSA Public Key Export	N/A	RSA public key with 2048 bits modulus size	Read
N/A	Initialization	N/A	N/A	N/A
CO	Key Generation (Symmetric key or RSA key pair generation)	HMAC_DRBG-SHA-256 with PR	32 bits DRBG Entropy input string, 256 bits V, 256 bits Key	Read, Write, Write
		RSA KeyGen	RSA public and private key pair with 2048 bits modulus size	Write
CO	DH Key Agreement (KAS FFC dhEphem with KDF)	KAS DH	256 bits Diffie-Hellman private key, 2048 bits Diffie-Hellman public key, 2048 bits Diffie-Hellman shared secret	Write, Write, Write
		One-step KDF	2048 bits Diffie-Hellman shared secret, 256 bits Derived Key	Read, Write
CO	Show Status	N/A	N/A	N/A
CO	On-Demand Self-Tests	N/A	N/A	N/A
CO	Zeroization (RAM or Flash)	N/A	RSA private key with 2048 bits modulus size, RSA public key with 2048 bits modulus size, 128 bits AES key, 256/512 bits HMAC key	Zeroize, Zeroize, Zeroize, Zeroize

Table 6 Service Authorized for Roles, Access Rights within Services

4.3 Authentication

This section is not applicable. Since the module meets FIPS 140-2 Security Level 1 requirements for this section, the User and Crypto Officer roles are implicitly assumed depending on the service used. No further authentication is required.

Role	Type of Authentication	Authentication Data
User	N/A	N/A
CO	N/A	N/A

Table 7 Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism

N/A	N/A

Table 8 Strength of Authentication Mechanisms

5. Physical Security

This section is not applicable. The FAST C-LIB is software only module.

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

Table 9 Inspection/Testing of Physical Security Mechanisms

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 10 Mitigation of Other Attacks

6. Operational Environment

6.1 Applicability

The FAST C-LIB operates in a modifiable operational environment per FIPS 140-2 Security Level 1 specifications. The module runs on a GPC as specified in Table 2: Tested Platform.

6.2 Policy

- The operating system is restricted to a single operator; i.e. concurrent operators are explicitly excluded. The application that requests cryptographic services is the single operator (User or CO) of the module.
- Self-Test functionality automatically performs when the module is loaded into memory, without any operator intervention. Refer to 10. Self-Tests for more information about Self-Test.

7. Cryptographic Key Management

When the FAST C-LIB performs cryptographic services, services that access keys and other CSPs (e.g. key zeroization) cannot run.

NOTE: Refer to APPENDIX B and APPENDIX C for more information about CSPs and public keys.

7.1 Random Number Generation

The FAST C-LIB uses a FIPS 140-2 approved deterministic random bit generator (DRBG) based on [SP 800-90A] for the generation of Keys/CSPs.

The module uses a true random number generator (TRNG) HW module embedded in Infineon AURIX HSM as the entropy source for seeding the DRBG.

Algorithm	HW module	Usage	Type
NDRNG	TRNG (embedded in Infineon AURIX HSM)	DRBG entropy input string (entropy strength: 256 bits)	Non-approved but allowed

Table 11 NDRNG Description

7.2 Key Generation

The module implements symmetric key generation using a HMAC_DRBG-SHA-256 with PR compliant with [SP 800-90A]. For generating RSA and DSA key pairs, the module implements asymmetric key generation services compliant with [FIPS 186-4].

The module does not output any data such as intermediate value during key generation process.

7.3 Key Establishment

The module implements Diffie-Hellman key agreement scheme with One-step KDF. Diffie-Hellman compliant with [SP 800-56Ar3] and One-step KDF compliant with [SP 800-56C].

As a result of Diffie-Hellman, shared secret of 2048 bits is calculated. The shared secret is inputted into the KDF, and then resulting a derived key of 256 bits.

7.4 Key Entry and Output

The module does not support manual key entry.

The module does not output intermediate key generation values. The module does not provide any symmetric key or private key output. The module only provides public key output.

7.5 Key Storage

RAM is volatile memory, so all data stored in RAM is not retained after power reset. FLASH is non-volatile memory, so all data stored in FLASH is retained after power reset.

NOTE: FLASH is encrypted by Infineon software with AES-CBC which is treated as plain text by FIPS 140-2 IG 1.23. Infineon software performs AES-CMAC sequence for integrity testing which is treated as plain text by FIPS 140-2 IG 1.23.

- All intermediate values such as DRBG internal state are ephemerally stored in RAM.
- All intermediate values such as DH host public key, DH shared secret, and KDF are ephemerally stored in RAM.
- The AES/HMAC/CMAC key and RSA key pair can be generated, established and then stored in FLASH.

7.6 Key Zeroization

The zeroization function overwrite the memory (RAM or FLASH) occupied by the keys and CSPs with "zeros (0)" and deallocate the memory.

- All intermediate values such as DRBG internal state are ephemeral and are zeroized when ended the appropriate DRBG process.
- All intermediate values such as DH host public key, DH shared secret, and KDF are ephemeral and are zeroized when ended the appropriate DH process.
- The AES/HMAC/CMAC key and RSA key pair stored in FLASH is zeroized when CO calls zeroization service for these key.

The module does not output any data during key zeroization process.

8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module cannot be certified by the FCC because it is not a standalone device nor a hardware component. Rather, it is designed to be embedded into a set of electronic products which themselves would undergo standard EMI/EMC certification. Please see FCC exemption below:

Title 47: Telecommunication PART 15 - RADIO FREQUENCY DEVICES Subpart B - Unintentional Radiators §15.103 Exempted devices. (a) A digital device utilized exclusively in any transportation vehicle including motor vehicles and aircraft.

9. Self-Tests

The FAST C-LIB performs FIPS 140-2 self-tests to ensure the integrity of the module and the correctness of the cryptographic algorithms.

9.1 Power-Up Self-Tests

The Power-Up Self-Tests functionality is performed upon power on, without operator intervention. While the module is performing the Power-Up Self-Tests, no cryptographic service is available and all data output is inhibited. If all the Power-Up Self-Tests are completed successfully, when the user role is set, the module enters the user state and cryptographic services for user role are available. When the CO role is set, the module enters the CO state and cryptographic services for CO role are available. If any failure occurs, the module enters fatal error state. In fatal error state, all data output is inhibited and no cryptographic service is available.

9.1.1 Software Integrity Test

The module's Software Integrity Test is performed using HMAC with SHA-256 compliant with [FIPS 198]. If the test successed, then the module automatically performs Cryptographic Algorithm Tests. If the test fails, then the module enters fatal error state.

9.1.2 Cryptographic Algorithm Tests

The module performs self-tests on all FIPS-Approved cryptographic algorithms supported in the approved mode of operation, using the known answer test (KAT) or Pair-wise Consistency Test (PCT) shown in the following table:

Algorithm	Test	Error Code
AES	KAT AES(ECB) with 128-bit key, encryption KAT AES(ECB) with 128-bit key, decryption	0xFFFF8001
	KAT AES(CBC) with 128-bit key, encryption KAT AES(CBC) with 128-bit key, decryption	0xFFFF8002
	KAT AES(CTR) with 128-bit key, encryption KAT AES(CTR) with 128-bit key, decryption	0xFFFF8004
	KAT AES(GCM) with 128-bit key, encryption KAT AES(GCM) with 128-bit key, decryption	0xFFFF8008
CMAC	KAT AES(CMAC) with 128-bit key, generate MAC KAT AES(CMAC) with 128-bit key, verify MAC	0xFFFFF001
HMAC	KAT HMAC-SHA-256	0xFFFF4001
	KAT HMAC-SHA-512	0xFFFF4002

SHA	KAT SHA-256	0xFFFF1001
	KAT SHA-512	0xFFFF2001
RSA	KAT RSA PKCS1.5 with 2048-bit modulus size, using SHA-256, generate sign KAT RSA PKCS1.5 with 2048-bit modulus size, using SHA-256, verify sign	0xFFFFF101
	KAT RSA PSS with 2048-bit modulus size, using SHA-256, generate sign KAT RSA PSS with 2048-bit modulus size, using SHA-256, verify sign	0xFFFFF101
DRBG	DRBG Health Tests as per [SP 800-90A] Section 11.3 are performed for all options described below: • HASH_DRBG-SHA-256 with PR • HASH_DRBG-SHA-256 without PR • HASH_DRBG-SHA-512 with PR • HASH_DRBG-SHA-512 without PR	0xFFFF0004
	DRBG Health Tests as per [SP 800-90A] Section 11.3 are performed for all options described below: • HMAC_DRBG-SHA-256 with PR • HMAC_DRBG-SHA-256 without PR • HMAC_DRBG-SHA-512 with PR • HMAC_DRBG-SHA-512 without PR	0xFFFF0001
DH	KAT DH with 2048-bit key, generate private parameter KAT DH with 2048-bit key, generate secret symmetric key	0xFFFFF201
KDF	KAT One-step KDF without Key Confirmation (Concatenation, SHA-256)	0xFFFFF201

Table 12 Power-Up Self-tests - Cryptographic Algorithm Tests

9.1.3 Critical Function Tests

No other critical function test is performed on power-up.

9.2 Conditional Tests

The module performs the following conditional self-tests:

Algorithm	Test	Error code
NDRNG	Continuous Random Bit Generator Test	0xFFFF000F
DRBG	Hash DRBG Continuous Random Bit Generator Test	0xFFFF0002

	Hmac DRBG Continuous Random Bit Generator Test	0xFFFF0008
RSA	PKCS1 V1.5 Sign/Verify Pairwise Consistency Test	0xFFFFF102
	PSS Sign/Verify Pairwise Consistency Test	0xFFFFF102
DH	DH Conditional Self-Tests (SP 800-56Ar3 conformant computation)	0xFFFFF202

Table 13 Conditional Tests

9.3 On-Demand Self-Tests

The module supports command-based on-demand self-tests service. The on-demand self-tests service is available only crypto officer (CO). The user cannot use this service.

The application can optionally run a specific self-tests or all tests on-demand by calling OnDemandTest() API. If the on-demand self-tests fail, the module enters fatal error state. In fatal error state, all data output is inhibited and no cryptographic service is available.

10. Mitigation of Other Attacks

This section is not applicable. The FAST C-LIB was not designed to mitigate any other attacks beyond the FIPS 140-2 Security Level 1 requirements.

APPENDIX A: SECURITY RULES

1. The module enforces logical separation between all data inputs, data outputs, control inputs, and status outputs via the cryptographic module API.
2. The module inhibits all data output during self-tests and error states.
3. Power-up self-tests do not require any operator intervention. While the module is performing the power-up self-tests, no cryptographic service is available and all data output is inhibited.
4. Power-up self-tests may be initiated on demand by power-cycling the module or the Crypto Officer can call power-up self-tests on demand.
5. The module support User role and Crypto Officer role.
6. The module does not support authentication mechanism.
7. The module does not support a maintenance interface or maintenance role.
8. The module does not support manual key entry.
9. The module does not support a bypass capability.
10. The module does not support a Software Load Test.
11. The module supports FIPS-Approved mode operation only.
12. The module protects CSPs from unauthorized disclosure, unauthorized modification, and unauthorized substitution.
13. The module does not output intermediate key values.
14. The module does not utilize non-56Arev3 functionality in the approved mode of operation.

APPENDIX B: CSPs

1. AES Key

Description	128-bit AES keys in the specific modes: ECB, CBC, CTR, GCM
Generation	SP800-90A HMAC_DRBG; As per SP 800-133 Section 7.1, key generation is performed as per the "Direct Generation" of Symmetric Keys which is an Approved Key generation method
Establishment	SP800-56Arev3 Diffie-Hellman, SP800-56C One-step KDF
Entry	N/A
Output	N/A
Storage	Plaintext in RAM, Plaintext in Flash
Key-to-Entity	Key usage flag - ECB: KEY_USAGE_AES128_ECB - CBC: KEY_USAGE_AES128_CBC - CTR: KEY_USAGE_AES128_CTR - GCM: KEY_USAGE_AES128_GCM
Zeroization	actively overwriting memory as a zero value (both RAM and Flash per a key)
Summary of protection	CRC check for protecting tampering

2. CMAC Key

Description	128-bit AES CMAC keys
Generation	SP800-90A HMAC_DRBG; As per SP 800-133 Section 7.1, key generation is performed as per the "Direct Generation" of Symmetric Keys which is an Approved Key generation method
Establishment	SP800-56Arev3 Diffie-Hellman, SP800-56C One-step KDF
Entry	N/A
Output	N/A
Storage	Plaintext in RAM, Plaintext in Flash
Key-to-Entity	Key usage flag - CMAC Generate/Verify: KEY_USAGE_AES128_CMAC
Zeroization	actively overwriting memory as a zero value (both RAM and Flash per a key)
Summary of protection	CRC check for protecting tampering

3. HMAC Key

Description	HMAC key with the following key sizes: - For HMAC-SHA-256: 256 bits

	- For HMAC-SHA-512, 512 bits
Generation	SP800-90A HMAC_DRBG; As per SP 800-133 Section 7.1, key generation is performed as per the "Direct Generation" of Symmetric Keys which is an Approved Key generation method
Establishment	SP800-56Arev3 Diffie-Hellman, SP800-56C One-step KDF
Entry	N/A
Output	N/A
Storage	Plaintext in RAM, Plaintext in Flash
Key-to-Entity	Key usage flag - HMAC-SHA-256 Generate/Verify: KEY_USAGE_HMAC256 - HMAC-SHA-512 Generate/Verify: KEY_USAGE_HMAC512
Zeroization	actively overwriting memory as a zero value (both RAM and Flash per a key)
Summary of protection	CRC check for protecting tampering

4. RSA Private Key

Description	2048-bit RSA private key for RSA digital signature generation operation
Generation	As per SP 800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method. The random value used in the key generation is generated using SP 800-90A HMAC_DRBG.
Establishment	N/A
Entry	N/A
Output	N/A
Storage	Plaintext in RAM, Plaintext in Flash
Key-to-Entity	Key usage flag - For RSA V1.5 Signature Generation: KEYUSAGE_RSA2048_V15_SIGNGEN - For RSA V2.1 Signature Generation: KEYUSAGE_RSA2048_V21_SIGNGEN
Zeroization	actively overwriting memory as a zero value (both RAM and Flash per a key)
Summary of protection	CRC check for protecting tampering

5. Diffie-Hellman Private Key

Description	256-bit Diffie-Hellman private key
Generation	As per SP 800-133 Section 6.2, key pairs for key establishment is performed as per FIPS 186-4. The random value used in the DSA domain parameter generation is generated using SP 800-90A HMAC_DRBG.
Establishment	N/A
Entry	N/A

Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	Key usage flag: KEYUSAGE_DH_PRIV
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	CRC check for protecting tampering

6. Diffie-Hellman Shared Secret

Description	2048-bit Diffie-Hellman shared secret
Generation	Generated using SP800-56Ar3 Finite Field Cryptography Diffie-Hellman (FFC DH) Primitive
Establishment	SP800-56Arev3 Diffie-Hellman, SP800-56C One-step KDF
Entry	N/A
Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	Diffie-Hellman process
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	N/A

7. KDF

Description	256-bit derived key using one-step KDF
Generation	Generated using SP800-56Ar3 Key-Derivation Methods
Establishment	SP800-56Arev3 Diffie-Hellman, SP800-56C One-step KDF
Entry	N/A
Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	Diffie-Hellman process
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	N/A

8. HASH_DRBG internal state (V, C)

Description	Random seed bits HASH_DRBG using SHA-256/SHA-512 - For using SHA-256: 440-bit V and C - For using SHA-512: 888-bit V and C
Generation	Derived from entropy input
Establishment	N/A

Entry	N/A
Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	DRBG process
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	N/A

9. HMAC_DRBG internal state (V, Key)

Description	Random seed bits HMAC_DRBG using SHA-256/SHA-512 - For using SHA-256: 256-bit V and Key - For using SHA-512: 512-bit V and Key
Generation	Derived from entropy input
Establishment	N/A
Entry	N/A
Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	DRBG process
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	N/A

10. DRBG Entropy input string

Description	DRBG Entropy input string is based on hardware TRNG module (for a time 32-bit)
Generation	Generated internally using a hardware TRNG
Establishment	N/A
Entry	N/A
Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	DRBG process
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	N/A

APPENDIX C: Public Keys

1. RSA Public Key

Description	2048-bit RSA public key for RSA digital signature verification operation
Generation	As per SP 800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method. The random value used in the key generation is generated using SP 800-90A HMAC_DRBG.
Establishment	N/A
Entry	N/A
Output	The key is passed out of the module via API (RSAPubKeyExport) output parameters in plaintext.
Storage	Plaintext in RAM, Plaintext in Flash
Key-to-Entity	Key usage flag - For RSA V1.5 Signature Verification: KEYUSAGE_RSA2048_V15_SIGNVER - For RSA V2.1 Signature Verification: KEYUSAGE_RSA2048_V21_SIGNVER
Zeroization	actively overwriting memory as a zero value (both RAM and Flash per a key)
Summary of protection	CRC check for protecting tampering

2. Diffie-Hellman Public Key

Description	256-bit Diffie-Hellman public key
Generation	As per SP 800-133 Section 6.2, key pairs for key establishment is performed as per FIPS 186-4. The random value used in the DSA domain parameter generation is generated using SP 800-90A HMAC_DRBG.
Establishment	N/A
Entry	N/A
Output	The key is passed out of the module via API (DHGenKeypair) output parameters in plaintext.
Storage	Plaintext in RAM
Key-to-Entity	Key usage flag: KEYUSAGE_DH_PUB
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	CRC check for protecting tampering

3. Diffie-Hellman recipient Public Key

Description	256-bit Diffie-Hellman recipient public key
Generation	N/A

Establishment	N/A
Entry	The key is passed into the module via API (DHDeriveKey) input parameters in plaintext.
Output	N/A
Storage	Plaintext in RAM
Key-to-Entity	DH process
Zeroization	actively overwriting memory as a zero value (RAM only)
Summary of protection	N/A

APPENDIX D: Acronyms

Term	Description
AES	Advanced Encryption Standard (FIPS-197)
API	Application Programming Interface
CBC	Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code (SP 800-38B)
CSP	Critical Security Parameter
CTR	Counter
CO	Crypto Officer
DRBG	Deterministic Random Bit Generator (SP 800-90A)
ECU	Electronic Control Unit
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standards
FIPS 140-2 IG	Federal Information Processing Standards 140-2 Implementation Guidance
GCM	Galois/Counter Mode
GPC	General Purpose Computing system
HMAC	Key-hashed Message Authentication Code (FIPS 198-1)
HSM	Hardware Security Module
KAT	Known Answer Test
N/A	Not Applicable
NDRNG	Non-deterministic Random Number Generator
OEM	Original Equipment Manufacturer
OSEK/VDX OS	Operating System (OS) standard for automotive embedded system
RAM	Random-Access Memory
V2X	Vehicle to Everything