Broadcom, Inc.

BCM58202B0

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.2
Date: April 09, 2025

Table of Contents

List of Tables

List of Figures

*				

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version BCM58202PB0KFBG10 of the BCM58202B0. It contains the security rules under which the module must operate and describes how

this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 3 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows from Table 1:

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

Table 1: Security Levels

1.3 Additional Information

The Module is a highly integrated SoC (System on a Chip). It is marketed with part number BCM58202PB0KFBG10 and is ideally suited for end point security protection applications.

2 – Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated cryptographic based security systems to protect sensitive information, access, usage, of computer, telecommunication systems, and property. The Module is intended to be used in commercial personal computers, point of sales terminals, access control devices in physically or electronically access restricted areas.

Module Type: Hardware

Module Embodiment: SingleChip

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1. The Module is a single-chip embodiment. The cryptographic module is encapsulated in an opaque and tamper resistant package material. The cryptographic boundary is the outer perimeter of the IC packaging.

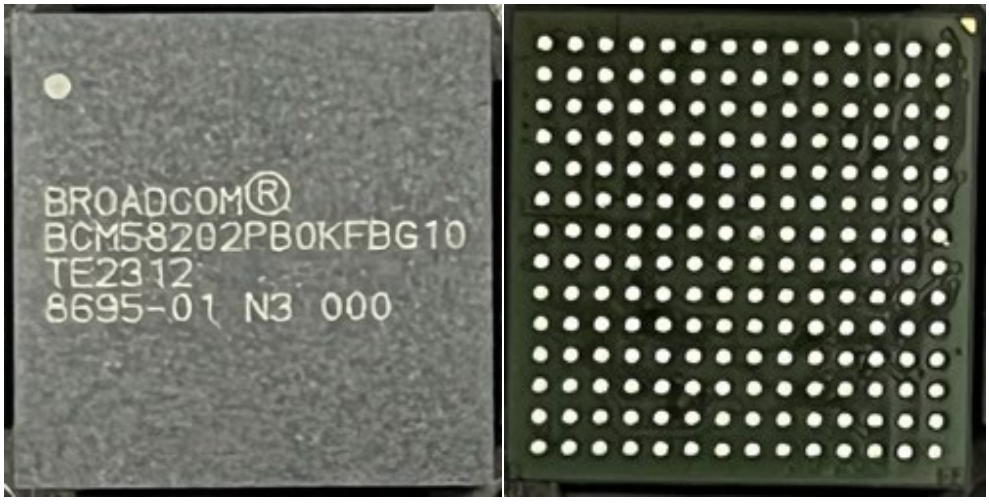

Figure 1 – [Model 1]

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

BCM58202B0 cryptographic module is tested with the following configuration.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
BCM58202B0	BCM58202PB0KFBG10	SBL Version: 1.1 SBI Version: 1.0 AAI Version: 2.1	BCM58202B0	BCM58202B0 single-chip SoC

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There were no components that were excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module only supports an Approved mode of operation.	Approved	RESET_OUT_L is high and UART prints the message, “The Device is running in FIPS operational mode: 0xFFFF

Table 3: Modes List and Description

The BCM58202B0 cryptographic module only supports an Approved mode of operation and does not support a non-Approved mode of operation. The module cannot be configured to operate in a non-compliant state. The Cryptographic Officer (CO) can confirm the Approved mode of operation when the status output RESET_OUT_L is high and UART prints the message, “The Device is running in FIPS operational mode: 0xFFFF”.

In addition, the CO can confirm they are using the appropriate version of the module by consulting the output of the "Get info" service:

Global Indicator (4)
Global Indicator: 00 00 ff ff
SBL Version (2)
SBL Version: 01 01
SBI Version (2)
SBI Version: 01 00
AAI Version (2)
AAI Version: 02 01
CHIP Version: BCM58202PB0KFBG10

BCM58202B0 is configured during manufacturing to operate in the Approved mode. The CO is responsible for confirming the appropriate versions of the SBI and AAI are loaded; no additional configuration is required.

2.5 Algorithms

Approved Algorithms:

The Module implements the Approved cryptographic algorithms listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	AES 5895	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	AES 5896	Key Length - 128, 192, 256	SP 800-38C
AES-CTR	AES 5895	Key Length - 128, 192, 256	SP 800-38A
AES-ECB	AES 5895	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
Counter DRBG	A3753	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
DSA SigGen (FIPS186-4)	A4437	L - 2048 N - 256 Hash Algorithm - SHA2-256	FIPS 186-4
DSA SigVer (FIPS186-4)	A4437	L - 2048 N - 256 Hash Algorithm - SHA2-256	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3751	Curve - P-256 Secret Generation Mode - Extra Bits	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyVer (FIPS186-4)	A3751	Curve - P-256	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3751	Component - No Curve - P-256, P-384 Hash Algorithm - SHA2-256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3751	Component - No Curve - P-256, P-384 Hash Algorithm - SHA2-256	FIPS 186-4
HMAC-SHA2-256	HMAC 3870	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3751	Domain Parameter Generation Methods - P-256 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KDA OneStepNoCounter SP800-56Cr2	A3752	Key Length - Key Length: 256	SP 800-56C Rev. 2
RSA SigGen (FIPS186-4)	A3750	Signature Type - PKCS 1.5 Modulo - 2048, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3750	Signature Type - PKCS 1.5 Modulo - 2048, 4096	FIPS 186-4
SHA2-256	SHS 4646	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA3-224	SHA-3 60	-	FIPS 202
SHA3-256	SHA-3 60	-	FIPS 202
SHA3-384	SHA-3 60	-	FIPS 202
SHA3-512	SHA-3 60	-	FIPS 202

Table 4: Approved Algorithms

KAS [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant key agreement scheme where testing is performed end-to-end for the shared secret computation and a KDA compliant with SP800-56Cr2 without key confirmation.

Vendor-Affirmed Algorithms:

The Module implements the Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG-Sym	Capabilities:Sections 4 and 6.1 Direct symmetric key generation using unmodified DRBG output; Section 6.2.1 Derivation of symmetric keys from a key agreement shared secret	DRBG (A3753)	SP800-133r2, IG [D.H]
CKG-Asym	Capabilities:Sections 4 and 5.1 Asymmetric signature key generation using unmodified DRBG output; Sections 4 and 5.2 Asymmetric key establishment key generation using unmodified DRBG output	ECDSA KeyGen (A3751)	SP800-133r2, IG [D.H]

Table 5: Vendor-Affirmed 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
AKG	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation	Publications:FIPS 186-4, SP800-90A, IG C.A, IG C.E	CKG-Asym Curve: P-256 ECDSA KeyGen (FIPS186-4) Counter DRBG
AKV	AsymKeyPair-KeyVer	Asymmetric Key-Pair Verification	Publications:FIPS 186-4, SP800-90A, IG C.A, IG C.E	ECDSA KeyVer (FIPS186-4) Curve: P-256
DPG	AsymKeyPair-DomPar	Domain Parameters	Publication:SP800-56Ar3	KAS-ECC-SSC Sp800-56Ar3 Curve: P-256 Counter DRBG

Name	Type	Description	Properties	Algorithms
DRBG	DRBG	Random Number Generation	Publication:SP800-90A	Counter DRBG Capabilities: AES-256 w/ Derivation Function
ENC	BC-UnAuth	Block Cipher	Publication:FIPS 197, SP800-38A	AES-CBC Key Size: 128, 192, 256 AES-CTR Key Size: 128, 192, 256 AES-ECB Key Size: 128, 192, 256
ENC-AUTH	BC-Auth	Authenticated Block Cipher	Publication:FIPS 197, SP800-38C	AES-CCM Key Size: 128, 192, 256
CKG-Symmetric	CKG	Symmetric Key Generation	Publication:IG D.H, FIPS 197, SP800-133r2 Sections 4 and 6.1 Direct symmetric key generation using unmodified DRBG output	Counter DRBG Key Size: 128, 192, 256
SigGen	DigSig-SigGen	Digital Signature Generation	Publication:FIPS 186-4, SP800-90A, FIPS 180-4	DSA SigGen (FIPS186-4) Key Size: 2048 ECDSA SigGen (FIPS186-4) Curve: P-256, P-384 RSA SigGen (FIPS186-4) Key Size: 2048, 4096 SHA2-256 Counter DRBG
SigVer	DigSig-SigVer	Digital Signature Verification	Publication:FIPS 186-4, SP800-90A, FIPS 180-4	DSA SigVer (FIPS186-4) Key Size: 2048 ECDSA SigVer (FIPS186-4) Curve: P-256, P-384 RSA SigVer

Name	Type	Description	Properties	Algorithms
				(FIPS186-4) Key Size: 2048, 4096 SHA2-256 Counter DRBG
ESV	ENT-ESV	Entropy Source	Publication:SP800-90B, IG 9.3.A, IG D.J, IG D.O	Counter DRBG Security Strength: 256
KAS	KAS-Full	Key Agreement	Publication:SP800-56Ar3, SP800-56Cr2 Caveat:Key establishment method provides 128 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3 Scheme: Ephemeral Unified (Responder) Curve: P-256 KDA OneStepNoCounter SP800-56Cr2 Auxiliary Function: SHA2-256 Key Length: 128 Counter DRBG
KTS	KTS-Wrap	Key Transport - Wrapping	Publication:FIPS 197, SP800-38F, IG D.G Caveat:Key establishment methodology provides 128 bits of encryption strength	AES-CCM Key Size: 128
MAC	MAC	Message Authentication Code	Publication:FIPS 198-1, FIPS 180-4, IG C.B	HMAC-SHA2-256 Capabilities: Key size < Block size
SHS	SHA	Secure Hash Standard	Publication:FIPS 180-4, FIPS 202, IG C.B, IG C.C	SHA2-256 Message Length: 0 - 51200 Increment 8 SHA3-224 Message Length: 0 - 51200 Increment 8 SHA3-256 Message Length: 0 - 51200 Increment

Name	Type	Description	Properties	Algorithms
				8 SHA3-384 Message Length: 0 - 51200 Increment 8 SHA3-512 Message Length: 0 - 51200 Increment 8

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

The module does not have any algorithm specific information.

2.8 RBG and Entropy

Cert Number	Vendor Name
E35	broadcom

Table 7: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
E35	Physical	BCM58202B0	32 bits	Minimum of 4 bits	N/A

Table 8: Entropy Sources

The entropy source produces 4 bits of entropy per 32 bit sample. When instantiating the DRBG, the module will collect a total of 3072 bits from the entropy source, which has a total of 384 bits of entropy. Per SP800-90Arev1, the module must provide security_strength bits of entropy (i.e., 256-bits) plus another security_strength/2 (i.e., 128-bits) to instantiate a CTR_DRBG to a security strength of 256 bits.

2.9 Key Generation

For Key Generation methods, see Section 2.6 Security Function Implementations above.

2.10 Key Establishment

Key Agreement Information

For Key Establishment methods, see Section 2.6 Security Function Implementations above.
The module supports KAS-ECC per SP800-56Ar3 using the Ephemeral Unified scheme with the NIST-recommended curve P-256, as tested under CAVP Cert. #A3751. The module employs the SP 800-56Cr2 OneStepKDF, which was validated under CAVP Cert. #A3752. No key confirmation is supported.

Key and seed generation is performed in compliance with NIST SP 800-133r2, Section 4, per 140-3 IG D.H without any post-processing. ECDSA Key Generation was tested under CAVP Cert. #A3751 using extra random bits, whereby an extra 64 bits are generated from the Approved DRBG (CAVP Cert. #A3753.
Full public key validation is performed according to SP 800-56Ar3, Section 5.6.2.3.3, on both the generated public key, as well as any received public key.
All temporary values used during the key agreement process are zeroized after the shared key is established.

Key Transport Information

For Key Transport methods, see Section 2.6 Security Function Implementations above.

2.11 Industry Protocols

The module does not implement any Industry Protocols>

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated defined logical interface categories are listed below.

The BCM58202B0 chip has a total of 141 signal pins. Each BCM58202B0 Interface Group listed below contains several BCM58202B0 pins. Unused Interface Groups will be marked as "Disabled" because they are disabled by the cryptographic module. The Module does not provide control output to other cryptographic modules or peripherals performing any cryptographic operations.

Physical Port	Logical Interface(s)	Data That Passes
Clock group	Control Input Status Output	Clock - 26MHz clock - 32KHz clock; Clock output - 26MHz clock output
Reset group	Control Input Status Output	One reset input; Reset output: Indicates that system power supply is stable.
Zeroisation	Control Input Status Output	Zeroisation request input (MANU_DEBUG)
SPI group	Data Input	Code and data from SPI flash (clock, device select, and four data I/O). All Code/Data Input is authenticated by the module.
USB group	Data Input Data Output Control Input Status Output	Service request input; Service response output; (USB differential data bus); Device interface used by the CO to make service requests. Requests are authenticated via the KAS secure session.
UART group	Status Output	Status output (Four UART ports of four signals each.)
Power group	Power	Over 50 power and ground pins. Power is distributed to the chip using designated IO and core power pins that are completely separated from any signal pin groups. Power pins are only connected to the internal power planes of the silicon chip.
Alert	Data Input	Tamper, Voltage, or Temperature event

Table 9: Ports and Interfaces

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Authentication is accomplished via a 256-bit ECDSA-based signature verification process using KOP-PUB. During the manufacturing process, the ECDSA private key, KDI-EC-PRIV, is loaded into SOTP of the Module and the corresponding public key, KDI-EC-PUB, resides in SRAM. KDI-EC-PUB is used to authenticate the module to the operator during the establishment of a secure session.
After an operator is authenticated successfully, the operator assumes the CO role. A secure session does not persist across power cycles. The Cryptographic Officer must be authenticated to establish a secure session before any cryptographic services are rendered.

In addition to the CO, the Module supports services which do not require authentication, listed as UA in Approved Services table.
The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators. The role of the CO is authenticated via the establishment of a mutually authenticated KAS session with ECDSA-based signatures. CO authentication is not carried over a terminated secure session or power cycle. A new secure session requires a complete CO authentication process.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Signature Verification	The CO role is authenticated by the verification of an ECDSA digital signature using a P-256 key.	SigVer	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^128 which is less than 1/1,000,000.	Based on performance limitations, the probability of successfully authenticating to the module within one minute is 3,750/2^128 which is less than 1/100,000. The module will only allow one attempt to verify the CO – if that attempt fails, the module will be in an error state and must be rebooted to try and become operational again

Table 10: Authentication Methods

4.2 Roles

The Module supports a single distinct operator role, the Cryptographic Officer (CO).

The Roles Table below lists all operator roles supported by the Module.

The Module does not support concurrent operators.

The CO's Public Key is installed in the SBI. It is protected with the SBI signature. SBI is also integrity protected with a CRC32 checksum. Only one CO public key is present in the SBI.

The BCM58202B0 Cryptographic Module supports a single operator role: Cryptographic Officer. Only the authorized operator can establish a secure session with the cryptographic module. The cryptographic module implements identity-based operator authentication to allow only the authorized operator to access cryptographic services.
Authentication is accomplished via a 256-bit ECDSA-based signature verification process. A single 256-bit ECDSA public key is embedded in the SBI. The 256-bit ECDSA public key is used to authenticate the CO during the establishment of a secure session between the module and the CO on the external host system.

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer	Identity	CO	Signature Verification

Table 11: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Info	Show module, versions, global indicator informa	"Succeeded"; "Failed"	None=	Return Module ID (ECDSA public key). Information returned to CO: Module Info Dump Global Indicator: (4)	None	Cryptographic Officer - KDI-EC-PUB: R Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	tion and Status			Global Indicator: 00 00 ff ff SBL Version: (2) SBL Version: 01 01 SBI Version: (2) SBI Version: 01 00 AAI Version: (2) AAI Version: 02 01 CHIP Version: BCM58202PB0 KFBG10		- KDI-EC-PUB: R
Symmetric_encrypt	Symmetric encryption of plaintext message	"Succeeded"; "Failed"	Input data, input size, key, key size, mode of operation Input : 128 bit blocks of plaintext Key size: 128, 192, 256 bit Modes: ECB, CBC, CTR	Return the ciphertext or an error status	ENC	Cryptographic Officer - KAPP-AES: E
Symmetric_decrypt	Symmetric decryption of ciphertext	"Succeeded"; "Failed"	Encrypted input data, input size, key, key size, mode of operation Input : 128 bit blocks of ciphertex	Return the plaintext or an error status	ENC	Cryptographic Officer - KAPP-AES: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			t Key size : 128, 192, 256 bit Modes : ECB, CBC, CTR			
Symmetric_key_gen	Generate AES or HMAC key in selected key slot	“Succeeded”; “Failed”	Selection of AES or HMAC key slot for key gen	Key generation complete status	DRBG CKG-Symmetric ESV	Cryptographic Officer - DRBG-EI and Seed: G,E - DRBG-State: G,E - KAPP-AES: G - KAPP-HMAC: G
Symmetric_key_import	Load AES or HMAC key in selected key slot	“Succeeded”; “Failed”	Selection of AES or HMAC key slot for key import	Load status	KTS	Cryptographic Officer - KAPP-AES: W - KAPP-HMAC: W - KKAS-SS: E
Asymmetric_sig_gen	Generate signature	“Succeeded”; “Failed”	Key/Curve size, private key, plaintext message	Digital signature of message	SigGen	Cryptographic Officer - KAPP-PRIV: E
Asymmetric_sig_ver	Signature verification	“Succeeded”; “Failed”	Key/Curve size, public key, signature	Status of signature verification	SigVer	Cryptographic Officer - KAPP-PUB: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Asymmetric_key_gen	Generate ECDSA P-256 Key Pair	"Succeeded"; "Failed"	Key slot	Key generation complete status	AKG AKV DPG DRBG ESV	Cryptographic Officer - DRBG-EI and Seed: G,E - DRBG-State: G,E - KAPP-PRIV: G,E - KAPP-PUB: G,E
Asymmetric_key_import	Load RSA, ECDSA, DSA keys	"Succeeded"; "Failed"	Asymmetric Public/Private Keys	Load status	KTS	Cryptographic Officer - KAPP-PRIV: W - KAPP-PUB: W - KKAS-SS: E
Secure_session	Establish a secure session with the CO by generating a shared key	"Succeeded"; "Failed"	Public Keys	Module's KAS public key	AKG AKV DPG DRBG ENC-AUTH SigGen SigVer KAS	Cryptographic Officer - KDI-EC-PRIV: E - KKAS-PRIV: G,E - KOP-PUB: E - KKAS-PUB: G,R - KKAS-OP-PUB: W,E - KSS: G,E - KKAS-SS: G,E - DRBG-State: G,E - DRBG-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						EI and Seed: G,E
Zeroise	Destroy all CSPs	Device Inoperative	None	Device Inoperative	None	Cryptographic Officer - KDI-EC-PRIV: Z
HMAC-SHA2-256	Generates MAC of input message	"Succeeded"; "Failed"	HMAC key, plaintext message	MAC of message	MAC	Cryptographic Officer - KAPP-HMAC: E
SHA3 hashing	Generates SHA3 digest	"Succeeded"; "Failed"	Digest size: 224, 256, 384, 512 bit Plaintext message	Digest of message	SHS	Cryptographic Officer
SHA2-256 hashing	Generates SHA2-256 digest	"Succeeded"; "Failed"	Digest size: 256 bit Plaintext message	Digest of message	SHS	Cryptographic Officer
Get Random Number	Request a random number	"Succeeded"; "Failed"	None	Random number	DRBG ESV	Cryptographic Officer - DRBG-EI and Seed: G,E - DRBG-State: G,E
Get Error Log	Get self-test error log	Three latest self-test errors and CRC checksum of error log	None	Error Log: the last three detected errors and the CRC checksum	None	Cryptographic Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Firmware Load	Load firmware from an external source at power-on	No error reported on service execution; Module accepts CO requests	Firmware images, signatures	Self-test results from SBI execution.	SigVer	Unauthenticated - KSBI: W,E - KAAI: W,E

Table 12: Approved Services

4.4 Non-Approved Services

All approved services implemented by the Module are listed in the table below:

NOTE: There are no Non-Approved services available.

4.5 External Software/Firmware Loaded

The module supports external firmware loads per IG 10.3.F, Additional Comment #3A. Both the Secure Boot Image (SBI) and Authenticated Application Image (AAI) are externally loaded into the module during initialization at every power-on. Each externally loaded image must have a valid ECDSA or RSA signature verified before the image is accepted. The hash of the public keys used to validate the candidate images are loaded prior to the firmware images themselves. The public keys are embedded in the SBI and AAI headers respectively. The hash of the embedded keys are validated against the preloaded hash values.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following firmware components:

- SBL : Incorporated in on-chip ROM, immutable
- SBI : Secure Boot Image, in binary, validated by SBL
- AAI : Authenticated Application Image, in binary, validated by SBI

SBI and AAI are loaded from companion external flash at every power-on; they are both signed, and CRC protected in the companion external flash device when the Module is powered down. SBI and AAI installation in the companion flash memory is performed during manufacturing. The module will automatically retrieve the SBI and AAI images for validation and load.

Upon powering up of the Module, SBL validates the SBI signature before SBI execution and SBI validates AAI signature before AAI is loaded and executes. SBI and AAI perform a CRC-32 integrity test of their respective executable image. SBI is validated with an ECDSA P-384 signature upon load and AAI is validated with an RSA 2048-bit signature upon load. Once validated, both SBI and AAI perform a 32-bit CRC integrity check upon execution.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycling the Module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The Module has a limited operational environment under the FIPS 140-3 definitions.
The Module includes a firmware load service using ECDSA and RSA to support necessary updates. Firmware versions validated to FIPS 140-3 will be explicitly identified on a validation certificate issued by the CMVP. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Physical Security

7.1 Mechanisms and Actions Required

The BCM58202B0 Cryptographic Module is a single chip device offering the following physical security mechanisms:

- The module package is of production-grade packaging material and uses standard passivation techniques.
- The module is enclosed in a hard, opaque, tamper resistant and evident enclosure.
- CO can periodically examine the device package for visual evidence of tampering like, scratch marks.
- There is no opening on the package for service or ventilation purposes.
- No tamper-evident seal is required on the Module package.
- Asserting the MANU_DEBUG signal will zeroize all SSPs in non-volatile memory (OTP), overwriting them with 1s. Zeroisation is executed in hardware and complete in microseconds.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-resistant IC packaging	6 months	Review for evidence of tamper. If tamper evidence is observed, zeroise the module.

Table 13: Mechanisms and Actions Required

7.5 EFP/EFT Information

The nominal operating temperature of the module is 0C to 70C. The nominal voltage range is 3.0V to 3.6V.

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-50C	EFT	Shutdown
HighTemperature	130C	EFT	Shutdown
LowVoltage	1.5V	EFT	Shutdown
HighVoltage	3.8V	EFT	Shutdown

Table 14: EFP/EFT Information

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	0C
HighTemperature	70C

Table 15: Hardness Testing Temperatures

8 Non-Invasive Security

At present, SP800-140F does not define any non-invasive attack mitigation methods and as such, this section is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Only stored in volatile memory (RAM).	Dynamic
OTP	Stored in One-Time Programmable memory	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
KAS-Entry	Outside	RAM	Plaintext	Automated	Electronic	KAS
KTS	Outside	RAM	Encrypted	Automated	Electronic	KTS
PT-Entry	Outside	RAM	Plaintext	Manual	Electronic	
PT-Output	RAM	Outside	Plaintext	Manual	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroisation Service (MANU_DEBUG pin). Contents of OTP are overwritten with all '1'	Permanently remove sensitive parameters by writing all '1'. No new data can be loaded.	Asserting the MANU_DEBUG signal
Z2	Zeroised by Power cycle or hard reset.	Remove temporary or generated sensitive data from being carried over to the next operating session.	Power cycle
Z3	Zeroise after Secure Session is established.	To prevent leakage of Secure Session secrets.	No operator intervention is needed.

Table 18: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG-EI and Seed	CTR_DRBG entropy input	3072 - 256	DRBG - CSP	ESV		DRBG
DRBG-State	CTR_DRBG internal state (V and Key)	256 - 256	DRBG - CSP	DRBG		DRBG
KKAS-PRIV	Private key for share secret generation	P-256 - 128	Asymmetric - CSP	AKG		KAS
KDI-EC-PRIV	Signing key of messages during secure session establishmen	P-256 - 128	Asymmetric - CSP	Installed during manufacturing.		SigGen
KAPP-AES	Encryption/decryption operations	128, 192, 256 - 128, 192, 256	Symmetric - CSP	CKG-Symmetric		ENC
KAPP-HMAC	Integrity operations	256 - 256	Symmetric - CSP	CKG-Symmetric		MAC
KAPP-PRIV	General purpose key for sig-gen	DSA: 2048, RSA 2048, 4096; ECDSA: P-256, P-384 - 112-192	Asymmetric - CSP	AKG		SigGen
KKAS-SS	AES-CCM secure session key.	128 - 128	Symmetric - CSP		KAS	ENC-AUTH KTS
KSS	Shared secret for session key derivation.	256 - 256	Symmetric - CSP		KAS	KAS
KDI-EC-PUB	Used by the CO to mutually authenticate the secure session.	P-256 - 128	Asymmetric - PSP	AKG		
KKAS-PUB	Ephemeral public key from Module for shared secret establishment	P-256 - 128	Asymmetric - PSP	AKG		KAS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KKAS-OP-PUB	Ephemeral KAS public key of the CO used to establish a secure session.	P-256 - 128	Asymmetric - PSP			KAS
KAPP-PUB	General purpose key for sig-ver.	DSA: 2048, RSA 2048, 4096; ECDSA: P-256, P-384 - 112-192	Asymmetric - PSP	AKG		SigVer
KOP-PUB	Public key to authenticate the CO during secure session establishment	P-256 - 128	Asymmetric - PSP			SigVer
KSBI	Public Key. SBI signature verification	P-384 - 192	Asymmetric - Neither			SigVer
KAAI	Public Key. AAI signature verification	2048 - 112	Asymmetric - Neither			SigVer

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI and Seed		RAM:Plaintext	Until use completes	Z2	DRBG-State:Initializes
DRBG-State		RAM:Plaintext	Until use completes	Z2	DRBG-EI and Seed:Derived From KKAS-PRIV:Generates KKAS-PUB:Generates KAPP-AES:Generates KAPP-HMAC:Generates KAPP-PRIV:Generates KAPP-PUB:Generates

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KKAS-PRIV		RAM:Plaintext	Until use completes	Z2 Z3	KKAS-SS:Derives KKAS-PUB:Paired With DRBG-State:Generated from
KDI-EC-PRIV		RAM:Plaintext OTP:Plaintext	Until use completes	Z1	KDI-EC-PUB:Paired With
KAPP-AES	KTS	RAM:Plaintext	Until use completes	Z2	DRBG-State:Generated from
KAPP-HMAC	KTS	RAM:Plaintext	Until use completes	Z2	DRBG-State:Generated from
KAPP-PRIV	KTS	RAM:Plaintext	Until use completes	Z2	KAPP-PUB:Paired With DRBG-State:Generated from
KKAS-SS		RAM:Plaintext	Until use completes	Z2	KSS:Derived From
KSS		RAM:Plaintext	Until use completes	Z2 Z3	KKAS-PRIV:Derived From KKAS-PUB:Derived From KKAS-OP-PUB:Derived From KKAS-SS:Derives
KDI-EC-PUB	PT-Output	RAM:Plaintext	Until use completes	Z2	KDI-EC-PRIV:Paired With DRBG-State:Generated from
KKAS-PUB	PT-Output	RAM:Plaintext	Until use completes	Z2 Z3	KKAS-PRIV:Paired With KKAS-SS:Derives DRBG-State:Generated from
KKAS-OP-PUB	KAS-Entry	RAM:Plaintext	Until use completes	Z2 Z3	KSS:Derives
KAPP-PUB	KTS	RAM:Plaintext	Until use completes	Z2	KAPP-PRIV:Paired With DRBG-State:Generated from
KOP-PUB	PT-Entry	RAM:Plaintext	Until use completes	N/A	
KSBI	PT-Entry	RAM:Plaintext	Until use completes	N/A	
KAAI	PT-Entry	RAM:Plaintext	Until use completes	N/A	

Table 20: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Conditional self–tests are periodically performed by the Module every 10 minutes or by power cycling the Module. The Module accepts one service request at a time. The Module will postpone periodic self-testing while critical operations are in progress. The Module will process a service request after the periodic self-test in progress. The Module logs the latest three (3) self-test errors in the Module's persistent registers, preserved across reset cycles. The CO can consult the error log by invoking Get Error Log service.

The Module performs the following pre-operational self-tests in table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity	CRC-32	EDC	SW/FW Integrity	Module has not entered error state.	A CRC-32 is checked on SBI and AAI respectively before SBI and AAI executes.

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (AES 5895)	AES-128, 192 and 256 – CBC Encrypt	KAT	CAST	Test name displayed and module does not enter ES1	Encryption - Forward cipher function	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (AES 5896)	AES-128 - CCM Encrypt	KAT	CAST	Test name displayed and module does not enter ES1	Authenticated encryption	Power-On
Counter DRBG (A3753)	AES-256 CTR_DRBG	KAT	CAST	Test name displayed and module does not enter ES1	AES-256 CTR_DRBG instantiate, generate, and reseed KATs.	Power-On
DSA SigGen (FIPS186-4) (A4437)	2048-bit Signature Generation with SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	Signature Generation	Power-On
DSA SigVer (FIPS186-4) (A4437)	2048-bit Signature Verification with SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	Signature Verification	Power-On
ECDSA SigGen (FIPS186-4) (A3751)	P-256 SHA2-256 and P-384 SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	Signature Generation	Power-On
ECDSA SigVer (FIPS186-4) (A3751)	P-256 SHA2-256 and P-384 SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	Signature Verification	Power-On
KAS-ECC-SSC Sp800-56Ar3 (A3751)	KAS-SSC Ephemeral Unified Model, C(2,0, ECC CDH). P-256	KAT	CAST	Test name displayed and module does not enter ES1	KAS-SSC Shared Secret generation with P-256	Power-On
ECDSA KeyGen (FIPS186-4) (A3751)	P-256	PCT	PCT	Test name displayed and module does not enter ES1ECDSA P-521 Key Generation Pairwise Consistency Test	ECDSA Key Generation Sign/Verify Pairwise Consistency Test	ECDSA Key Generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ENT	SP800-90B Health Test	APT and RCT	CAST	Test name displayed and module does not enter ES1	An RCT and APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input	Continuous
Firmware Loading	ECDSA P-384 with SHA2-256 or RSA 4096 with SHA2-256	Signature Verification	SW/FW Load	Module does not enter ES1. Self-Tests initiate	Signature Verification using ECDSA P-384 (SBI) or RSA 4096 (AAI)	Upon firmware load
HMAC-SHA2-256 (HMAC 3870)	HMAC-SHA256 Key Sizes: $\lambda = 32$ bytes	KAT	CAST	Test name displayed and module does not enter ES1	HMAC-SHA2-256 KAT – Inclusive to SHA2-256 testing	Power-On
KDA OneStepNoCounter SP800-56Cr2 (A3752)	One step KDA with SHA2-256 in no counter mode. SP800-56c-rev2 One-Step Key Derivation Function, Section 4.1, Option 1	KAT	CAST	Test name displayed and module does not enter ES1	Generate 256-bits of keying material	Power-On
RSA SigGen (FIPS186-4) (A3750)	2048-bit and 4096-bit with SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	2048-bit and 4096-bit RSA PKCSv1.5 with SHA2-256 Signature Generation	Power-On
RSA SigVer (FIPS186-4) (A3750)	2048-bit and 4096-bit with SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	2048-bit and 4096-bit RSA PKCSv1.5 with SHA2-256 Signature Verification	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (SHS 4646)	SHA2-256	KAT	CAST	Test name displayed and module does not enter ES1	SHA2-256	Power-On
SHA3-224 (SHA-3 60)	SHA3-224	KAT	CAST	Test name displayed and module does not enter ES1	SHA3-224	Power-On
SHA3-256 (SHA-3 60)	SHA3-256	KAT	CAST	Test name displayed and module does not enter ES1	SHA3-256	Power-On
SHA3-384 (SHA-3 60)	SHA3-384	KAT	CAST	Test name displayed and module does not enter ES1	SHA3-384	Power-On
SHA3-512 (SHA-3 60)	SHA3-512	KAT	CAST	Test name displayed and module does not enter ES1	SHA3-512	Power-On
KAS Key Generation	KAC-ECC P-256. Ephemeral Unified	PCT	PCT	Secure session establishment proceeds and module does not enter ES1	Pairwise Consistency Test as defined by SP800-56Ar3.	KAS Key Generation
AES-CBC (AES 5895)	AES-128, 192 and 256 – CBC Decrypt	KAT	CAST	Test name displayed and module does not enter ES1	Decryption - Inverse cipher function	Power-On
AES-CCM (AES 5896)	AES-128 - CCM Decrypt	KAT	CAST	Test name displayed and module does not enter ES1	Authenticated decryption.	Power-On

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity	EDC	SW/FW Integrity	Ponwer-On	Automatically

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (AES 5895)	KAT	CAST	10 minutes	Automatically
AES-CCM (AES 5896)	KAT	CAST	10 minutes	Automatically
Counter DRBG (A3753)	KAT	CAST	10 minutes	Automtically
DSA SigGen (FIPS186-4) (A4437)	KAT	CAST	10 minutes	Automatically
DSA SigVer (FIPS186-4) (A4437)	KAT	CAST	10 minutes	Automatically
ECDSA SigGen (FIPS186-4) (A3751)	KAT	CAST	10 minutes	Automatically
ECDSA SigVer (FIPS186-4) (A3751)	KAT	CAST	10 minutes	Automatically
KAS-ECC-SSC Sp800-56Ar3 (A3751)	KAT	CAST	10 minutes	Automatically
ECDSA KeyGen (FIPS186-4) (A3751)	PCT	PCT	N/A	N/A
ENT	APT and RCT	CAST	Continuous	Automatically
Firmware Loading	Signature Verification	SW/FW Load	N/A	N/A
HMAC-SHA2-256 (HMAC 3870)	KAT	CAST	10 minutes	Automtically
KDA OneStepNoCounter SP800-56Cr2 (A3752)	KAT	CAST	10 minutes	Automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A3750)	KAT	CAST	10 minutes	Automatically
RSA SigVer (FIPS186-4) (A3750)	KAT	CAST	10 minutes	Automatically
SHA2-256 (SHS 4646)	KAT	CAST	10 minutes	Automatically
SHA3-224 (SHA-3 60)	KAT	CAST	10 minutes	Automatically
SHA3-256 (SHA-3 60)	KAT	CAST	10 minutes	Automatically
SHA3-384 (SHA-3 60)	KAT	CAST	10 minutes	Automatically
SHA3-512 (SHA-3 60)	KAT	CAST	10 minutes	Automatically
KAS Key Generation	PCT	PCT	N/A	N/A
AES-CBC (AES 5895)	KAT	CAST	10 minutes	Automatically
AES-CCM (AES 5896)	KAT	CAST	10 minutes	Automatically

Table 24: Conditional Periodic Information

Conditional self–tests are periodically performed by the Module every 10 minutes.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ESI	The Module fails a KAT, PCT, conditional or periodic self-test, FW integrity, critical function tests, DRBG self-tests.	The Module enters the FIPS error state	Reboot/Power cycle the module	The Module enters the FIPS error state and SBL fails to boot or continue operation, and enters a continuous reset loop.

Table 25: Error States

10.5 Operator Initiation of Self-Tests

Self-tests can be initiated by power cycling or issuing a reset to the Module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Module is manufactured and fully tested in secure environments under authorized access control. The Module is installed in the final product with the companion external flash device in the manufacturing facility.
The CO must ensure the appropriate versions of the SBI and AAI are loaded in the companion external flash device upon first power up of the Module using the "Get Info" service. The CO should also visually inspect the Module for tamper evidence.
The Module is a single chip device that does not provide any maintenance service access. At the end of life of the Module, all CSPs shall be zeroised by setting MANU_DEBUG pin high and power cycling the Module.

Installation and Initialization:

The following steps must be performed in order to securely install, initialize, and start up the BCM58202B0 cryptographic module in the FIPS 140-3 Approved mode of operation:

The Module should be installed in the final product with the companion external flash device in the manufacturing facility. The manufacturing process includes a Module customization step which installs SBI and AAI in the module, initializes the Module with per device unique AES and HMAC keys, binding the Module and the flash device.

The CO must ensure the appropriate versions of the SBI and AAI are loaded in the companion external flash device upon first power up of the Module using the “Get Info” service. The CO should also visually inspect the Module for tamper evidence.

Delivery:

The CO must ensure the appropriate versions of the SBI and AAI are loaded in the companion external flash device upon first power up of the Module using the “Get Info” service. The CO should also visually inspect the Module for tamper evidence.

11.2 Administrator Guidance

Before the Module is installed in the end product, the module package should be inspected for integrity and to be free of any tamper evidence.

The Module should be installed in the final product with the companion external flash device in a secure manufacturing facility. The manufacturing process includes a Module customization step which installs SBI and AAI in the module. To ensure the appropriate versions of the SBI and AAI are loaded in the companion external flash device, execute the “Get Info” service upon first power up of the Module. Verify the expected versions are reported.

While the Module is in service in the end product, it is recommended to perform a visual inspection of the Module at least every 6 months to ensure that the Module package is still intact and void of any tamper evidence. “Get Info” service should be run to ensure that the correct SBI and AAI versions are in operation.

Upon the termination of service of the Module, all critically sensitive parameters in the Module should be zeroized by setting the MANU_DEBUG pin high and power cycling the Module. Then, the Module can be disposed of responsibly.

11.3 Non-Administrator Guidance

Same as above for Administration Guidance.

11.4 Design and Rules

Rules of Operation

1. The Module provides one distinct operator roles: Cryptographic Officer.
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.

4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module does not output intermediate key values.
16. The Module does not provide bypass services or ports/interfaces.

11.5 Maintenance Requirements

The Module is a single chip device that does not provide any maintenance service access.

11.6 End of Life

At the end of life of the Module, all CSPs shall be zeroised by setting MANU_DEBUG pin high and power cycling the Module.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

References and Definitions

The following standards are referred to in this Security Policy.

Abbreviation*	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, August 1, 2023*
[108r1]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), August 2022*
[133r2]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Cr2]	*NIST Special Publication 800-56C Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, August 2020*
[90Ar1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*

References

Acronym*	Definition
APT	Adaptive Proportion Test
KAT	Know Answer Test
RCT	Repetition Count Test
SSP	Sensitive Security Parameter

Acronyms and Definitions