Application Note

NIST SP 800-90A Compliance for the CC23xx AESCTRDRBG Driver

Sam Hachem, Achyut Ray *Automotive Connectivity Solutions*

ABSTRACT

This application note documents the advanced encryption standard (AES) counter-based (CTR-based) deterministic random bit generator (AESCTRDRBG) driver shipped in the TI SimpleLink™ Secure Drivers package for the CC23xx device family and presents the compliance evidence for NIST SP 800-90A produced by the TI verification suite. The note also explains why NIST SP 800-90A is the applicable normative basis for evaluating a deterministic random bit generator (DRBG) such as the one implemented on CC23xx, rather than the statistical output test suite specified in NIST SP 800-22 Rev. 1a.

Table of Contents

Trademarks

1 Introduction

The CC23xx SimpleLink family provides an AES CTR-based deterministic random bit generator (AESCTRDRBG) driver that supplies deterministic random bit generation services to system integrators. This document captures three items required by end customers and OEM stakeholders:

- The mapping between the CC23xx AESCTRDRBG driver and the NIST SP 800-90A specification
- The methodology used to verify the driver against the NIST CAVP CTR_DRBG test vectors
- The full pass/fail results of the verification suite executed on 04-Apr-2025

2 Detailed Description

2.1 Scope

This note applies to the AESCTRDRBG driver in the TI Secure Drivers repository for the CC23xx family. This note covers the deterministic mechanism only. Physical entropy source characterization (NIST SP 800-90B) and RBG construction (NIST SP 800-90C) are outside the scope of this document.

2.2 Standard Selection: SP 800-22 versus SP 800-90A

SP 800-22 defines fifteen statistical tests on the bit stream output of an RNG. The applicable normative standard for a deterministic DRBG such as the CC23xx AESCTRDRBG driver is NIST SP 800-90A Rev. 1, not SP 800-22, for the following reasons:

1. SP 800-90A specifies the mechanism construction (CTR_DRBG, Hash_DRBG, HMAC_DRBG). SP 800-90A is the specification the driver implements, and is the specification against which conformance must be demonstrated.
2. NIST's cryptographic module validation program (CMVP) validates DRBGs under FIPS 140-3 against SP 800-90A/90B. SP 800-22 is not used in that validation process (see FIPS 140-3 Implementation Guidance).
3. SP 800-22 evaluates statistical properties of an output stream. Passing the SP 800-22 suite is a necessary-but-not-sufficient signal: cryptographically broken generators can and do pass the suite. Peer-reviewed analysis (Saarinen, PQShield, 2022) demonstrates this on the reference generators shipped with SP 800-22.
4. The CC23xx AESCTRDRBG driver is a deterministic mechanism that accepts an externally provided seed. The correctness of the driver is verifiable by known answer tests (KATs) against the NIST CAVP CTR_DRBG vectors, which is the mechanism SP 800-90A is validated with.

The evidence set in this note therefore uses SP 800-90A conformance through NIST CAVP CTR_DRBG vectors.

2.3 Device and Driver Under Test

Item	Value
Device family	CC23xx (SimpleLink Bluetooth® Low Energy Wireless MCU)
Driver	AESCTRDRBG (Secure Drivers package)
Mechanism	CTR_DRBG per NIST SP 800-90A Rev. 1, Section 10.2
Block cipher / key size	AES-128
SDK	Included in SimpleLink CC23xx SDK 9.20 (and back-ported to 9.11 through patch)
TF-M configuration under test	tfm_disabled

2.4 NIST SP 800-90A Feature Mapping

The table below maps SP 800-90A features to the CC23xx AESCTRDRBG driver. Optional features not required for the deterministic use case documented here are explicitly identified.

NIST SP 800-90A feature	Driver support	Notes
Mechanism	CTR_DRBG only	Hash_DRBG and HMAC_DRBG not implemented.
Derivation function (df)	No	Optional per SP 800-90A section 10.2.1.
Prediction resistance	No	Driver does not implement PR. CAVP PR-true vector set is therefore not applicable to this configuration.
Personalization string	Yes	Per SP 800-90A section 8.7.1.
Additional entropy input on Reseed	Yes	Per SP 800-90A section 9.2.
Additional data input on Generate	No	Optional per SP 800-90A §9.3.
Reseed interval	Configurable, enforced	Verified by dedicated test (see section 7).

2.5 Test Methodology

The verification infrastructure is built on the NIST CAVP DRBG Validation System (DRBGVS) specification. Test vectors are the publicly published CAVP CTR_DRBG vectors. The vectors are executed against every public-facing API of the driver, across all supported combinations of RTOS, toolchain, and return-behavior.

2.5.1 Vector Sets Applied

The vector sets used for testing can be found here:

- CTR_DRBG, no reseed (drbgvectors_no_reseed).
- CTR_DRBG, reseed without prediction resistance (drbgvectors_pr_false).
- CTR_DRBG with prediction resistance (drbgvectors_pr_true): not applicable - driver does not implement PR; excluded by design.

2.5.2 Build Matrix Executed

Axis	Values
RTOS	NoRTOS, FreeRTOS
Toolchain	IAR, GCC, Clang/LLVM
Return behaviour	Blocking, Polling
Key size	AES-128
TF-M	tfm_disabled (KeyStore path skipped and verified separately)

2.6 Test Coverage

Tests exercise the full public API surface of the AESCTRDRBG driver:

Table 2-1. Source: tests/secure_drivers/aesctrdrbg/general/tests/test_aesctrdrbg_general.py in the secure_drivers repository.

Test	Purpose
test_getRandomBytes	Validate raw random byte output against CAVP KATs
test_getBytes	Validate byte-level generation path
test_generateKey	Validate AES key generation derived from the DRBG
test_generateKeyWithKeyStore	KeyStore integration path (requires TF-M enabled; skipped in this run)
test_reseed_interval	Validate enforcement of the configured reseed interval per SP 800-90A section 9.3.1

2.7 Results

Aggregate outcome, report generated 04-Apr-2025:

Outcome	Count
Passed	48
Failed	0
Errors	0
Skipped (by design, TF-M off)	12
Total	60

The twelve skipped tests are all test_generateKeyWithKeyStore variants. The tests are skipped with reason "KeyStore APIs not supported in tfm_disabled configuration" and are covered by a separate execution when TF-M is enabled. All non-skipped tests pass across every (RTOS, toolchain, return-behaviour) combination in the matrix.

2.7.1 Per Axis Summary

RTOS	Toolchain	Blocking passed	Polling passed
NoRTOS	IAR	5 / 5	5 / 5
NoRTOS	GCC	5 / 5	5 / 5
NoRTOS	LLVM	5 / 5	5 / 5
FreeRTOS	IAR	5 / 5	5 / 5
FreeRTOS	GCC	5 / 5	5 / 5
FreeRTOS	LLVM	5 / 5	5 / 5

2.8 Bluetooth SIG Qualification Context

The Bluetooth SIG qualification test specification does not mandate RNG entropy statistical tests for either the Controller or Host layers. Bluetooth SIG explicitly delegates RNG suitability to the silicon manufacturer. This document provides the official proof that TI's CC23xx chip set meets the SP 800-90A security standard.

3 Test Vector File Mapping

The CAVP DRBG test vector distribution is a zip archive of .rsp files. The subset applied against the AESCTRDRBG driver is listed below. Full expected and actual comparison is performed by the pytest harness. A mismatch on any KAT produces a FAIL result in the report.

Archive	Applicable files	Applied?
drbgvectors_no_reseed.zip	CTR_DRBG.rsp (AES-128, no df)	Yes
drbgvectors_pr_false.zip	CTR_DRBG.rsp (AES-128, no df, reseed)	Yes
drbgvectors_pr_true.zip	CTR_DRBG.rsp (AES-128, PR)	No (feature not implemented)
drbgvectors_*	Hash_DRBG.rsp, HMAC_DRBG.rsp	No (mechanism not implemented)

4 Summary

The CC23xx AESCTRDRBG driver passes every applicable NIST CAVP CTR_DRBG test vector executed against its public API, across all supported RTOS/toolchain/return-behavior combinations. The driver conforms to the CTR_DRBG mechanism specified in NIST SP 800-90A Rev. 1 for the feature set documented in Section 2.4. This satisfies the applicable normative compliance basis for a deterministic DRBG used in a Bluetooth Low Energy platform.

5 References

1. NIST SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015. https://doi.org/10.6028/NIST.SP.800-90Ar1
2. NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018. https://doi.org/10.6028/NIST.SP.800-90B
3. NIST SP 800-22 Rev. 1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010. NIST Planning Note 2022-04-19: publication under revision. https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final
4. NIST CAVP DRBG Validation System (DRBGVS). https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/DRBGVS.pdf
5. NIST CAVP DRBG test vectors. https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/drbgtestvectors.zip
6. FIPS 140-3, Security Requirements for Cryptographic Modules, March 2019. https://doi.org/10.6028/NIST.FIPS.140-3
7. M-J. O. Saarinen. SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful. PQShield Ltd., 2022

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025