SP 800-90B Non-Proprietary Public Use Document

Document Version 1.5

Software Version 3.0

NetApp, Inc.
3060 Olsen Drive
San Jose, California 95128
USA

August 29, 2022

Revision History

Version	Change
1.0	First draft for NetApp, Inc. and CryptoMod v3.0
1.1	Revisions for CCOM1 comments.
1.2	Revisions for CCOM2 comments.
1.3	Revisions for NetApp. Inc. comments.
1.4	Revisions for CCOM3 comments.
1.5	Final updates based on vendor comments.

Table of Contents

Description

The NetApp CryptoMod v3.0 module implements the library from CPU Jitter RNG to obtain entropy for key generation in the module. The source is a non-physical (ENT (NP)) entropy source. The CPU Jitter RNG library v3.4.0 source was tested on ONTAP 9.11.1 OS running on Intel® Xeon® D-2164IT, Intel® Xeon® Silver 4210 and Intel® Xeon® Platinum 8352Y processors.

Security Boundary

The basic operation of the CPU Jitter RNG entropy source is shown in Figure 1. Timing jitter from memory access and hashing operations is collected and injected into the entropy pool for access by the module.

The entropy source is internal to the module as identified by the red dashed box showing the logical cryptographic boundary in the block diagram below (Figure 2). Output from the entropy source is used to seed a deterministic random bit generator (DRBG). The module implements a NIST SP800-90Arev1 Counter DRBG for the generation of random bits. All these components reside within the physical boundary of the hardware platform as shown by the black dashed box.

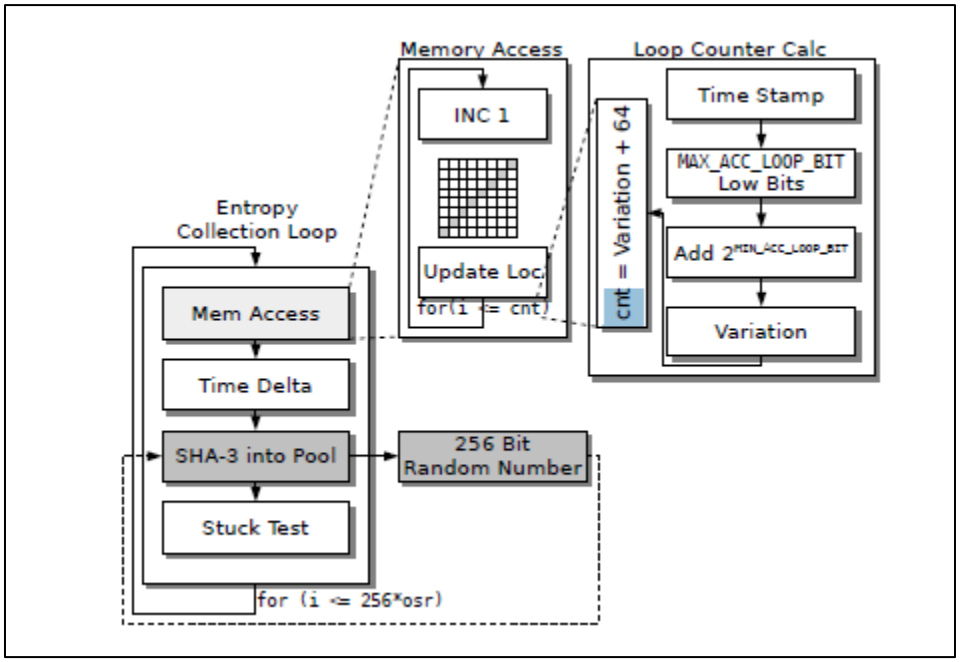

Figure 1 - Entropy source diagram

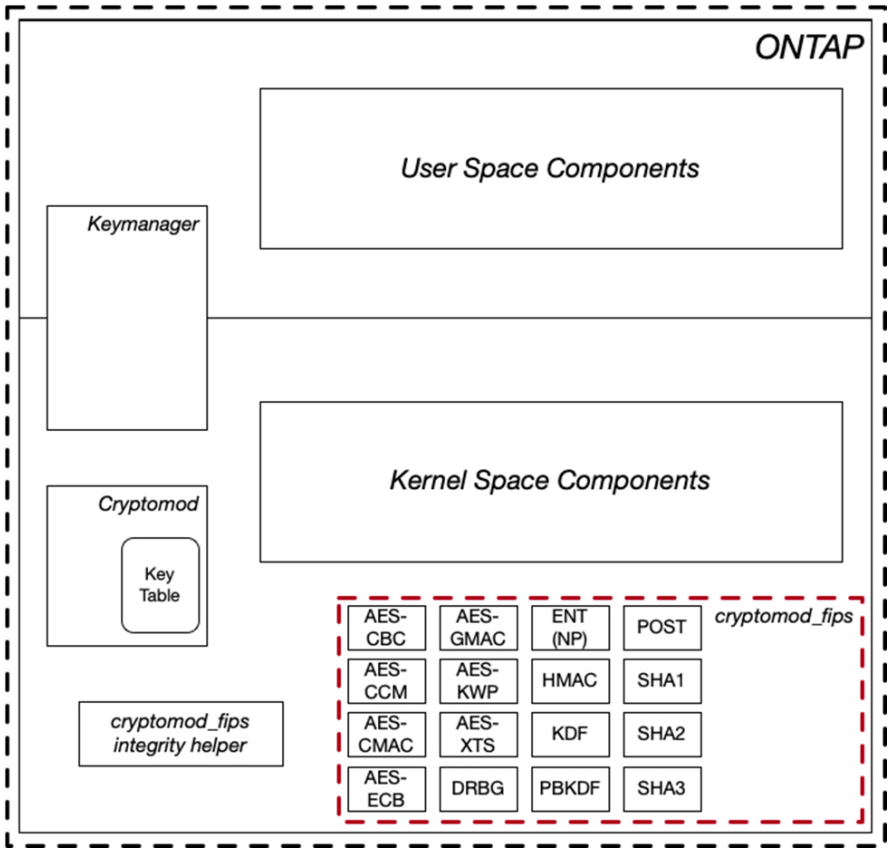

Figure 2 - Module Block Diagram

Operating Conditions and Configuration Settings

The following table summarizes operating conditions and compilation configuration settings.

Parameter	Value	Description
Temperature	0 °C – 78°C	Processor (s) temperature range.
Voltage	0.75V-1.35V	Processor (s) voltage range. VID (Voltage Identification)
Clock speed	2.10 GHz - 2.20 GHz	Processor clocking speed with impact on high-resolution timing required for CPU Jitter RNG.
Cache size	64 KiB	L1 cache size per core
Compilation Options (JENT v3.4.0)		
JENT_RANDOM_MEMACCESS	True	Enabled
JENT_MEMORY_BITS	17	Number of bits in a memory block (i.e., the memory block size in bits is 2^JENT_MEMORY_BITS)
JENT_MEMORY_SIZE	128KiB	Memory block size
JENT_MEMORY_ACCESSLOOPS	128	Memory access loops
JENT_MIN_OSR	3	Set by JENT_RANDOM_MEMACCESS

Parameter	Value	Description
JENT_CONF_DISABLE_LOOP_SHUFFLE	True	Disables pseudo-random looping e.g., lower boundary entropy equals upper boundary entropy.

The CPU Jitter RNG library was tested on ONTAP 9.11.1 OS running on Intel® Xeon® D-2164IT, Intel® Xeon® Silver 4210 and Intel® Xeon® Platinum 8352Y CPUs. All processors provide a high-resolution timer and default compilation options for CPU Jitter RNG v3.4.0 were used.

Physical Security Mechanisms

NetApp CryptoMod v3.0 is a Security Level 1 Software module within a Multiple-chip standalone embodiment. The module is implemented completely in software in such a manner that the physical security is provided solely by the computing platform.

Conceptual Interfaces

The GetEntropy interface is called during the instantiation function of the DRBG to provide the seed.

Min-Entropy Rate

The NetApp CryptoMod v3.0 entropy source provides 256 bits of min-entropy per 256-bit output sample, or full entropy.

Health Tests

The module continuously performs the Health Tests in SP 800-90B section 4.4 using the repetition count test (RCT) and adaptive proportion test (APT) as part of the module's conditional self-tests.

Maintenance

There are no specific maintenance requirements for the entropy source.

Required Testing

The entropy source continuously runs the SP 800-90B health tests and will produce an error upon failure.

In addition, raw sequential and restart data samples can be obtained from the entropy source for statistical testing using SP 800-90B test tools with the following requirements:

1. Raw noise data through the raw noise source interface and processed by the SP800-90B tool to obtain an entropy rate must be near equal to or the defined min-entropy rate.
2. Obtain the restart noise data through the raw noise source interface and processed by the SP800-90B tool.
    a. the sanity test to apply to the noise restart data must pass, and
    b. the minimum of the row-wise and column-wise entropy rate shall not be less than half of the entropy rate from 1 above.