SP 800-90B Non-Proprietary Public Use Document

Google's TRNG Entropy Source

Prepared by

EWA-Canada
1223 Michael St North, Suite 200
Ottawa, Ontario, K1J 7T2, Canada

On behalf of:

Google, LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
15th August, 2025

Revision History

Version	Change
1.0	Initial Draft
2.0	Adding on IN762 SoC C1
2.1	Finalized Draft
2.2	Minor correction to the table of contents.
2.3	Minor correction to table 1
2.4	ESVUP adding on 2 TRNGS for IN763 SoC A0

Table of Contents

Description 3
Security Boundary 5
Operating Conditions 6
Configuration Settings 6
Physical Security Mechanisms 6
Conceptual Interfaces 8
Entropy Rate 8
Health Tests 9
Maintenance 10
Required Testing 10

Description

Google's TRNG Entropy Source, is a hardware-based, physical (ENT (P)) entropy source. It is a non-IID entropy source. The Entropy Source is autonomous and does not require firmware or software to operate.

This assessment was conducted on the devices listed in Table 1 against the requirements from NIST's SP 800-90B published in January 2018 and those from FIPS 140-3 IG published in April 2025.

Table 1: Evaluated Entropy Source Specification

Entropy Operational Environment	Part Number / Platform	ECB Cert	Conditioner Cert	DRBG Cert
IN762 SoC B1	IN762 SoC	A2932	A2932	A2721
IN762 SoC C1[1]	IN762 SoC	A2932	A2932	A2721
IN763 SoC A0 IMC	IN763 SoC	C1278	A2272	C1278
IN763 SoC A0 SBB	IN763 SoC	C1278	A2272	C1278

The Google TRNG Entropy Sources are 32-bit instantiations of Synopsys DWC TRNG NIST B227 version 3.00b. The Synopsys CAVP CertificatesA2932 and A2721 are relevant to this submission.

For the ESVUP IN763 SoC Entropy-Operational Environments are 128-bit instantiations of Synopsys DWC TRNG NIST B227 version 3.00b. The Synopsys CAVP Certificates C2178 and C1278 are relevant to this submission.

Further the NIST SP800-90B TRNG Entropy Sources hardware design meets the criteria of SP800 90C-draft 4 to enable Cryptographic Modules to with additional firmware to implement compliant functionality.

[1] B1 and C1 are the stepping or version numbers of the die.

The IN762 SoC is a purpose specific Integrated Circuit (IC) shown in Figure 1, where the logic circuits were fabricated in a non-mutable manner. The TRNG Entropy Source provides a random number to the IMC sub-chip Cryptographic Module. A block diagram of the IC is shown below that shows two ARM A53 cores and other sub-chip Cryptographic Modules (ECM, LCE & ICE) on the same IN762 SoC die.

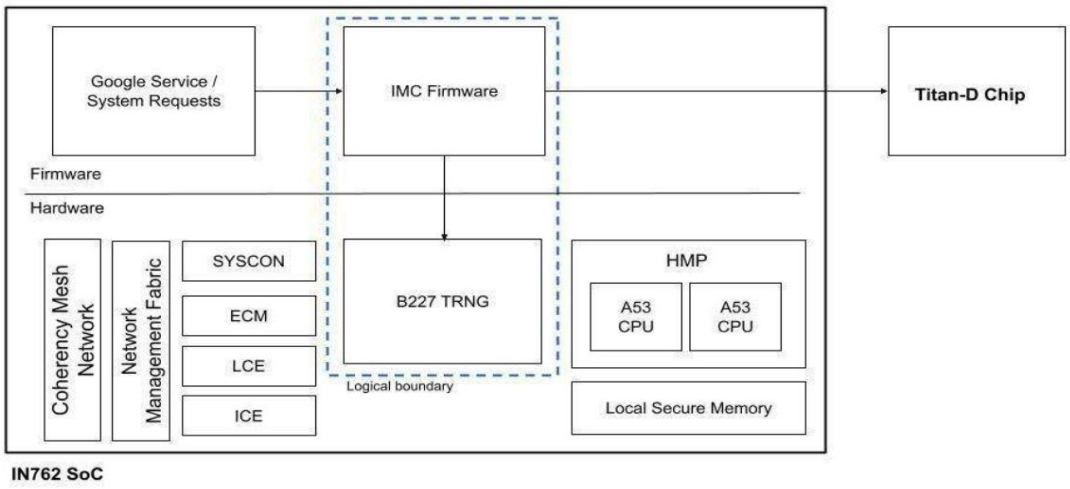


Figure 1: Conceptual view of IN762 SoC

The IN763 SoC is a purpose specific Integrated Circuit (IC) shown in Figure 2, where the logic circuits were fabricated in a non-mutable manner. The TRNG Entropy Source provides a random number to the Secure Firmware sub-chip Cryptographic Module. A block diagram of the IC is shown below that shows Integrated Compute Complex (ICC) and other sub-chip Cryptographic Modules (ECM, LCE, ICE & NVMe) on the same IN763 SoC die.

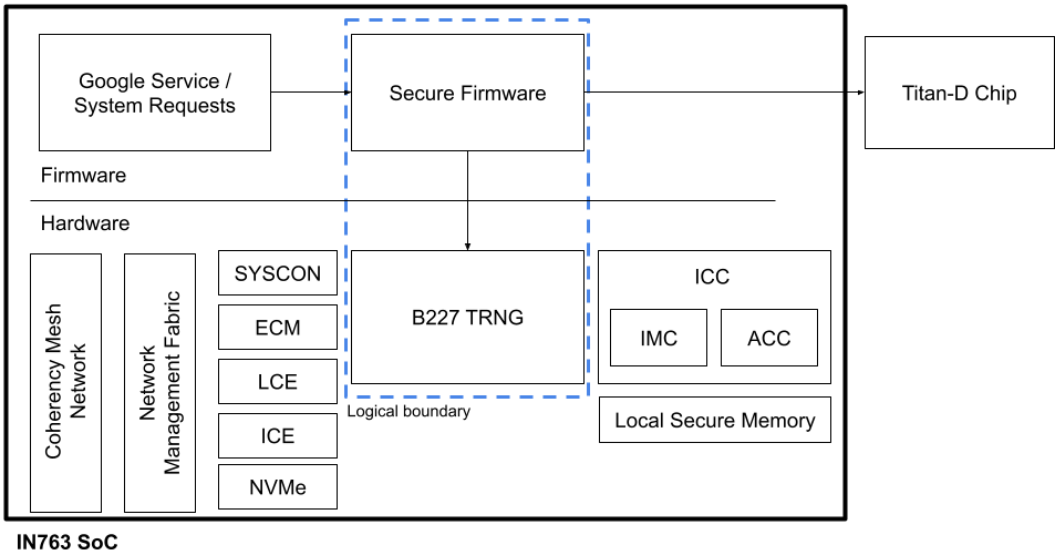


Figure 2: Conceptual view of IN763

Security Boundary

Google's TRNG Entropy Source consists of a noise source, conditioning component, and continuous health testing as shown in Figure 3. The noise source consists of bit generators which are based on a set of two ring oscillators per generator. The Entropy Source permits reading of the raw (unconditioned) output of the noise source only when in test mode. The vetted conditioning component is an AES-128 block_cipher_df (see Table 1 for each OE's corresponding CAVP certificate). The conditioned output is also available for input into a hardware-based DRBG (not shown) or may be read directly via registers. Continuous health tests are run on the raw noise data.

The security boundary is depicted in Figure 3 includes the DRBG as the RANDx registers are the only externally exposed interface for random number generation.

The implementation allows cryptographic module vendors to implement a RBG3(RS) according to the criteria of draft 4 of SP 800-90C as is set out in the Conceptual Interfaces section.

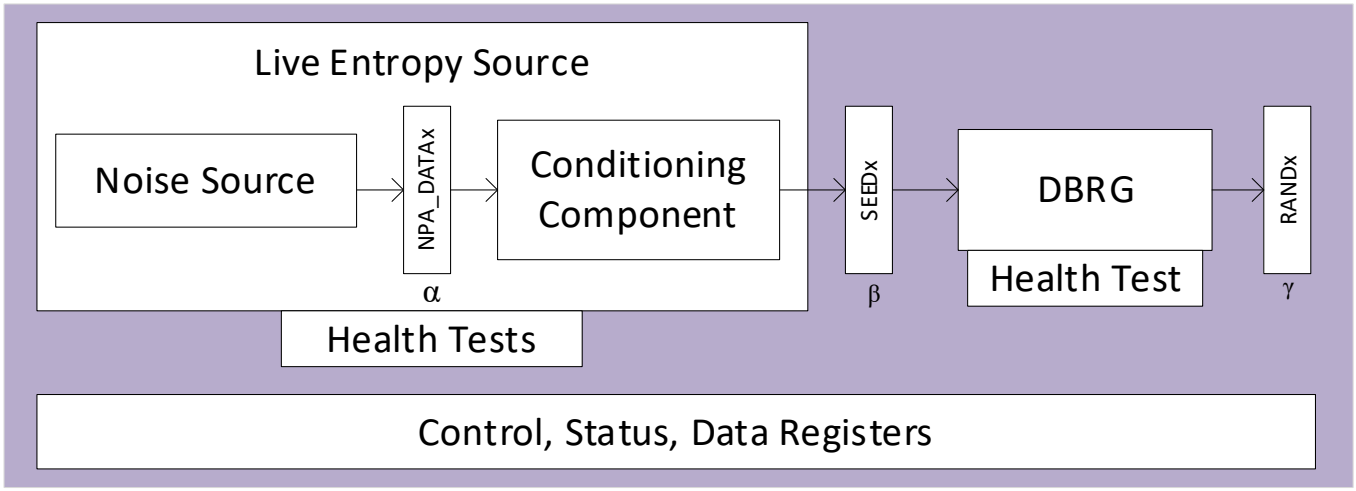


Figure 3: Google TRNG Entropy Source Block Diagram

The noise source itself consists of 6 or 8 bit-generators which are based on ring oscillators. Each bit generator comprises two ring oscillators and a digitizer. There is a single bit collector in the noise source.

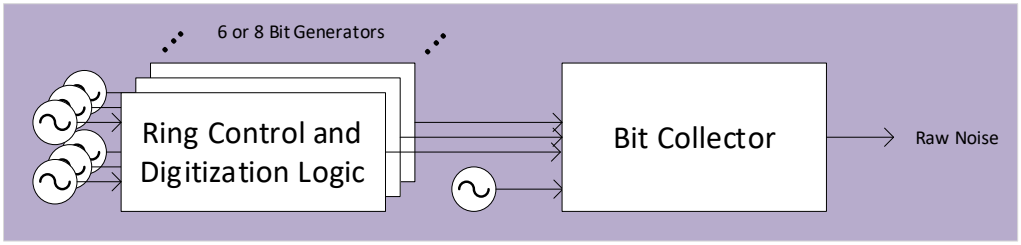


Figure 4: Noise Source Block Diagram

One round of KAT on the conditioning component and the DRBG plus a full round of statistical tests on the noise source are performed as the start-up test after reset. Control Interface Registers allow for test results to be checked and the request on-demand KAT testing of either or both the conditioner and the DRBG.

Operating Conditions

Table 2: Operating Conditions

Part Number	Temperature	Voltage
IN762 SoC	Min: 0C; Typical: 30C; Max: 105C	Range: 0.7V to 0.82V*
IN763 SoC	Min: 0C; Typical: 30C; Max: 100C	Range: 0.75V – 0.82V*

* The TRNG is on a fixed voltage supply per individual SOC, externally regulated and internally specified. So, voltage cannot be varied. During manufacturing, the test program searches for the minimum voltage (within reliability guardrails) necessary for that device to operate – this accounts for temperature and process corner. That minimum voltage is fused into the part. Testing occurred at this specific per-SOC voltage. For the aggregate of all SOCs, the voltage may range from 0.7V to 0.82V.

Configuration Settings

Google's TRNG Entropy Source does not require configuration of entropy-relevant parameters. Settings such as sample interval, startup delay, health test enable, etc. are all statically configured at build time and cannot be changed in the hardware.

Physical Security Mechanisms

Google's TRNG Entropy Source is embedded in the system on chip (SOCs) listed above. The SoCs are single-chip embodiments of production-grade components that include standard passivation. The SOCs are only usable when soldered to printed circuit board and are typically packaged using a ball grid array (BGA) package. The entropy source operates within the physical protections of the associated device package. This is capable of meeting FIPS 140-3 Level 1 or 2 requirements without additional security measures. Any required additional security measures such as tamper seals, etc. exist outside the package at the enclosure level. Any module integrating an SOC with Google's TRNG Entropy Source included within their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

The entropy source is only accessible by the internal processor which is typically running authenticated code. Direct access to the entropy source is not possible from any other interface. Zeroization of the TRNG including the entropy source occurs after reset and is available upon demand and may be triggered by internal processor within the SOC.

Conceptual Interfaces

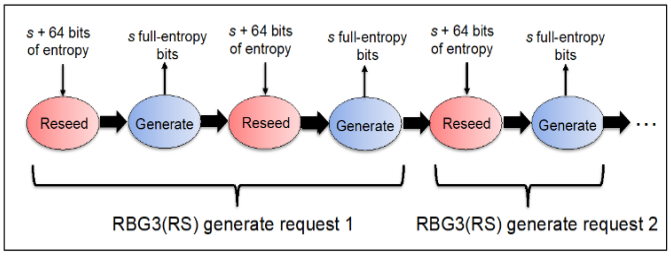
The Entropy Source exposes a set of instruction registers that enable the implementer of a Cryptographic module to generate random numbers using the SP800-90Ar1 approved DRBG.

The Entropy Source provides full entropy seed material for the DRBG.
The seed lengths exceed the DBRG security strength + 64 bits SP800-90C draft 4 requirements.
The seeds are not directly accessible except in test mode.

The Entropy source interface logic allows for reseed and Generate requests allow the Cryptographic Module to implement the following SP800-90C draft 4 constructs:

1. RBG2(P).
2. RBG3(RS) an achievable example from SP800-90C draft 4 is shown below:

Figure 8: RBG3 (RS) Generate Requests



Entropy Rate

The entropy source fully saturates the Block_Cipher_DF conditioning component, so the output of the entropy source has a min-entropy rate of 128-bits per 128-bit block (or full entropy).

Health Tests

Google's TRNG Entropy Source performs the NIST SP800-90B required health tests on the entropy source. One round of Known Answer Test (KAT/CAST) on the conditioning component plus a full round of statistical tests on the noise source are performed as the start-up test after reset. The number of noise bits that are generated and tested as part of the start-up test is 1024-bits. All bits generated and tested during the start-up test are discarded after the test regardless of the success or failure of the test. The entropy health test block receives bits coming out of the noise source and performs continuous statistical tests on those bits.

The continuous NIST SP800-90B health tests include:

- Repetition Count Test (RCT)
- Adaptive Proportion Test (APT)

The health tests always run during mission mode of operation. Health tests can only be individually disabled at runtime when the core is in test mode. In mission mode, health tests cannot be disabled. Any transition between test and mission modes, enables all health tests.

The following parameters are used for the RCT:

Parameter	Value
Sample size	1 bit
Min-Entropy	H=50%
Cutoff value	C=41
False positive error rate	Alpha = 2^{-20}

The following parameters are used for the APT:

Parameter	Value
Sample size	1 bit
Min-Entropy	H=50%
Cutoff Value	C=793
Window Size	w=1024
False positive error rate	Alpha = 2^{-20}

When a health test fails, whether it is statistical or KAT and whether during the start-up test, continuous statistical checks or on-demand testing, a non-maskable alarm rises and the core zeroizes itself. The cause of failure can be read from ALARMS register.

While the start-up test is ongoing, the core is in busy state and remains unfunctional until the start-up test is finished. If the test finishes successfully, the core is ready to be used.
If the start-up test fails, the TRNG issues an alarm and zeroizes itself. However, by default, the hardware comes out of the busy state and is ready to be used. It is the responsibility of the application software to take proper action upon failure. The software resets the core to kick-off a new round of start-up test if desired.

On-demand statistical test is possible by rebooting the core. Note that resetting, rebooting, or powering up are acceptable methods for initiating an on-demand test since the procedure results in the immediate execution of the start-up tests. Samples collected from the noise source during on demand health tests at startup time are discarded. Continuous statistical testing continues after the startup tests providing that there are no errors.

Maintenance

There are no maintenance requirements.

Required Testing

Google's TRNG Entropy Source was tested by placing the TRNG in test mode and collecting raw noise data through the raw noise data register. The non-IID SP800-90B tests using the most recent update of the NIST 90B test implementation were run over data collected. The non-restart assessment was run as well as the restart assessment. Test data was collected following the requirements of Section 3 of SP 800-90B. All tested data was evaluated at a higher entropy than the defined min entropy rate, all restart sanity checks passed, and both the row and column-wise entropy were nearly identical to the non-restart entropy value. No additional testing is required.