XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

# True Random Number Generator (TRNG)

Product code: XIP8001B

The TRNG IP core establishes a benchmark for hardware-based security in cryptographic systems, by generating high-entropy, true random numbers essential for secure communications and cryptographic operations, such as key generation. It includes a robust and thoroughly characterised entropy source, online health tests and a proven AES-CBC-MAC-based entropy extractor.

The IP core conforms to the stringent requirements of NIST standards and widely used test suites, while offering flexibility and broad compatibility for both FPGA and ASIC designs. It is an essential component of security protocols such as TLS 1.3 and MACsec.

## KEY FEATURES

- Moderate resource requirements
- Compliant with NIST SP 800-22 / SP 800-90B
- Ready for FIPS 140-3 certification
- AES-CBC-MAC-based entropy
- Security features (e.g. zeroise function)
- Passes PractRand, gjrand, TestU01, and dieharder test suites
- Parameterisable design
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

## APPLICATIONS

Enhance your security with high-entropy TRNG:

- Defense and military communications
- VPN / TLS / IPsec / MACsec implementations
- Automotive systems
- Wearables
- Space and satellite applications

## TRNG

*High-quality true random numbers*

The TRNG core integrates robust health monitoring systems to ensure the highest level of randomness and security under any operational conditions.

It includes advanced noise reduction techniques to optimise entropy quality, further strengthening against predictability and enhancing the system's cryptographic security.

### BALANCED

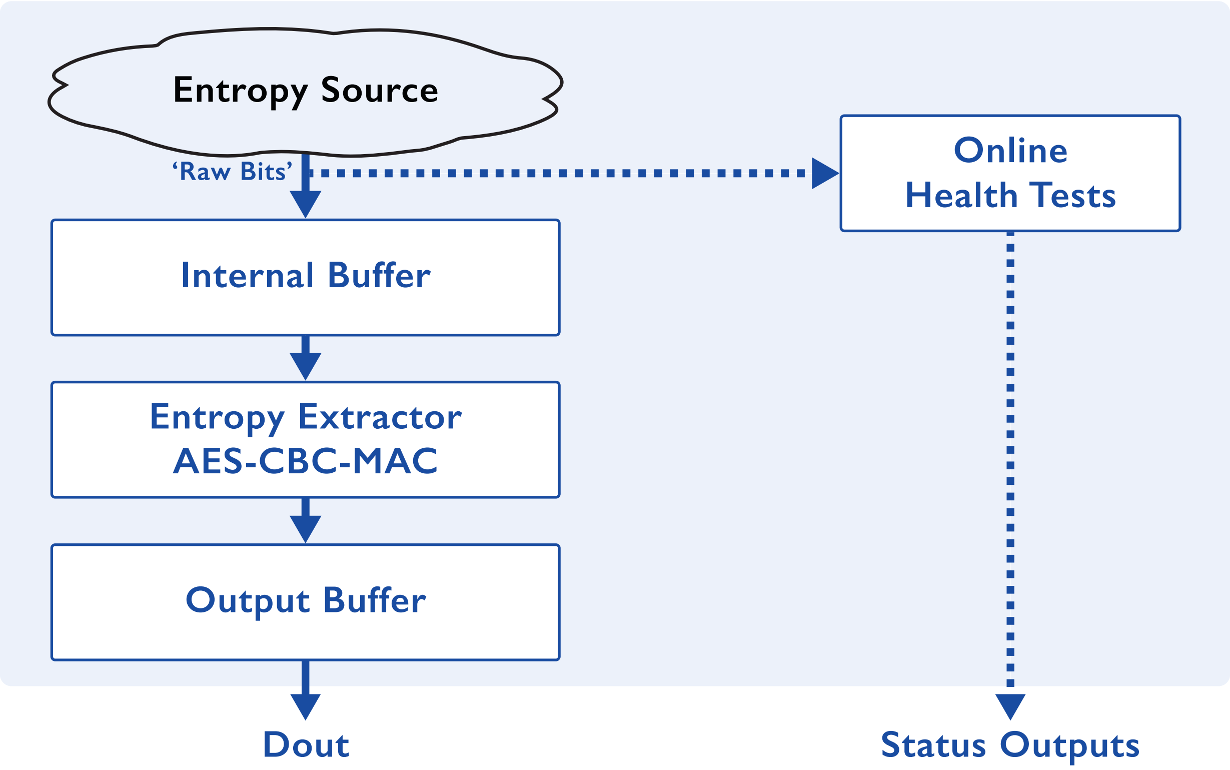
*XIP8001B*

- Moderate resource requirements with no multipliers or DSP blocks
- Tunable entropy source
- Additional security features
- Easily portable fully digital design

*Combining the TRNG with our NIST SP800-90A compliant PRNG provides a NIST SP800-90C compliant Random Number Generator, optimal for cryptographic security.*

XIPHERA

## True Random Number Generator (TRNG)



## Deliverables

| | |
|---|---|
| ✓ Encrypted RTL or source code | ✓ Optional netlist |
| ✓ Sample synthesis scripts | ✓ Instantiation file |
| ✓ Comprehensive simulation test bench, scripts & guide | ✓ Detailed datasheet and integration guide |
| ✓ Mathematical model of the entropy source | ✓ Test report |
| ✓ Testing guide | ✓ Implementation guide |
| ✓ Entropy source description | |

Product Flyer - TRNG - V1.0.1

### About Xiphera

Xiphera, Ltd, is a Finnish company designing hardware-based security solutions using standardised cryptographic algorithms. Our product portfolio consists of secure and efficient cryptographic Intellectual Property (IP) cores, designed directly for ASICs and FPGAs. Our strong cryptographic expertise, extensive experience in system design, and deep knowledge in the field of reprogrammable logic enable us to offer our customers peace of mind in a dangerous world.

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

Tekniikantie 12
02150 Espoo
Finland

Email: sales@xiphera.com
Phone: +358 20 730 5252
Web: www.xiphera.com