SECURE-IC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

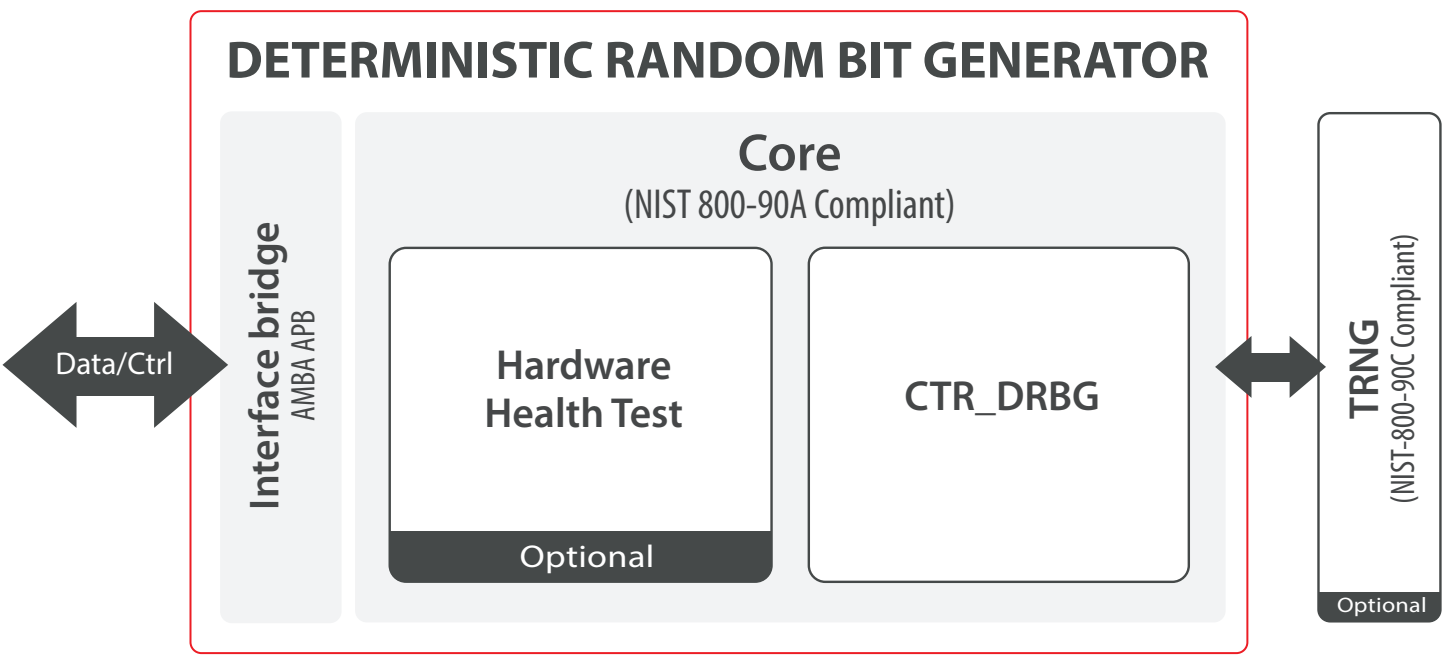
Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Secure IP > Key Management > SCZ_IP_DRBG

DETERMINISTIC RANDOM BIT GENERATOR (DRBG)

The Deterministic Random Bit Generator is an essential silicon-proven digital IP core for all FPGA, ASIC and SoC designs that targets cryptographically secured applications. It is a deterministic algorithm compliant with the NIST-800-90A Rev1. The IP Core successfully passed NIST-800-90A Rev1 test suites and it is compliant with the FIPS-140-2 validation.

Random number generation is critical for any secure device. Random numbers are used for key generation, key exchange, digital signature, encryption and more. Typical secure protocols like IPsec, MACsec, TLS/SSL or wireless use them during authentication/ key exchange and data streaming phases.

The Deterministic Random Bit Generator can be provided with the True Random Number Generator (TRNG) to have a full FIPS 140-2 compliant Random number Generator (NIST 800-90A/B/C). Convenient AMBA APB interface is used for both control and data transfer.



Features

- NIST 800-90A/B/C compliant
- FIPS 140-2 compliant
- AMBA APB interface
- Health test
- Ready for FIPS 140-3
- Pure digital
- AES-CTR based (CTR_DRBG)
- Portable to FPGA and ASIC technology

Applications

- Defense
- IoT
- IPSec (VPN)
- Wearable devices
- TLS/SSL
- Embedded Security
- Automotive
- HSM

Software Support

Linux drivers are available to ease the integration in Linux OS. The Linux driver provides direct access to the true random number generator through "/dev/random". Software driver for micro-controller application is also available to ease the control of the random generator.

Technology

The entropy source is completely digital without any specific technology-dependent implementation. It makes it easy to port it to any technology (all ASIC nodes, Intel and Xilinx FPGA families). The random generator has been used in many ASIC and FPGA designs. Products from our customers have also passed FIPS 140-2 validation.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking test-bench based on FIPS vectors
- Documentation

V4.0

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US
www.secure-ic.com