

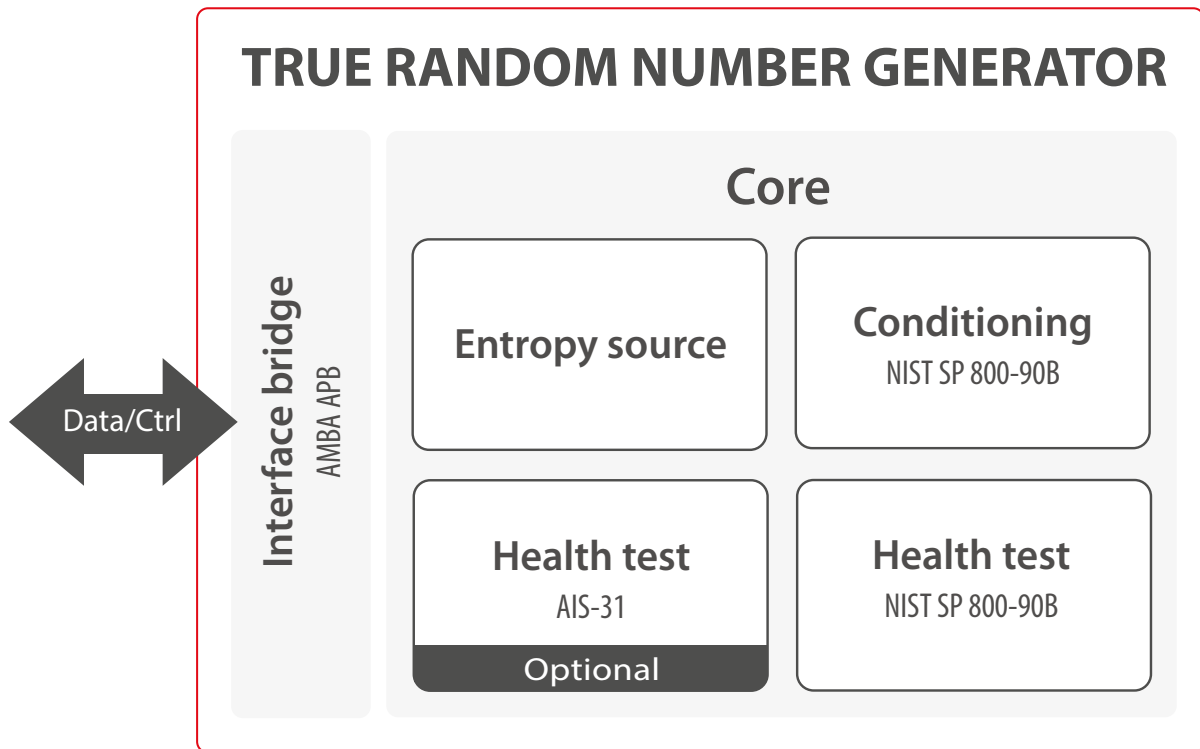
Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Secure IP > Key Management > SCZ\_IP\_BA431

# TRUE RANDOM NUMBER GENERATOR (TRNG)

The True Random Number Generator is an essential silicon-proven digital IP core for all FPGA, ASIC and SoC designs that targets cryptographically secured applications. It is a digital source of entropy designed for compliance with the NIST-800-90B and AIS31. The IP Core successfully passed NIST-800-22, 90B and AIS31 test suites on the entropy source 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 true random number generator includes conditioning function and health tests as defined in the NIST 800-90B and AIS31. Convenient AMBA APB interface is used for both control and data transfer.



Features			Applications	
✓ NIST 800-90B compliant	✓ FIPS 140-2 compliant	✓ Linux drivers (access from /dev/random)	✓ Defense	✓ IIoT
✓ AIS-31 start-up and on-line tests (optional)	✓ Ready for FIPS 140-3	✓ AMBA APB interface	✓ IPsec (VPN)	✓ Wearable devices
✓ Passed NIST 800-22, 90B and AIS31 test suites	✓ Portable to FPGA and ASIC technology	✓ Pure digital	✓ TLS/SSL	✓ Embedded Security
			✓ Automotive	

## 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 compilation
- ✓ Self-checking RTL test-bench based on FIPS vectors
- ✓ Documentation

V1.2

The True Random Number Generator is available in our **Deterministic Random Bit Generator** (SCZ\_IP\_BA433) and **Crypto Coprocessors** (SCZ\_IP\_BA450/456/457).

**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](mailto:contact@secure-ic.com)

**EMEA** |  
[sales-EMEA@secure-ic.com](mailto:sales-EMEA@secure-ic.com)

**AMERICAS** |  
[sales-US@secure-ic.com](mailto:sales-US@secure-ic.com)

**APAC** |  
[sales-APAC@secure-ic.com](mailto:sales-APAC@secure-ic.com)

**JAPAN** |  
[sales-JAPAN@secure-ic.com](mailto:sales-JAPAN@secure-ic.com)

**CHINA** |  
[sales-CHINA@secure-ic.com](mailto:sales-CHINA@secure-ic.com)

CONTACT US

[www.secure-ic.com](http://www.secure-ic.com)