# BarcoSilex

# Random Number Generator IP

BA431
Product sheet

**The Random Number Generator (BA431) is an essential silicon-proven digital IP core for all FPGA, ASIC and SoC designs that targets cryptographically secured applications.**

**The BA431 includes a True Random Generator (TRNG) as the source of entropy. The optional Deterministic Random Bit Generator (DRBG) can be provided with the core. The entropy source and the DRBG are designed for compliance with the NIST 800-90A and NIST 800-90B draft.**

**It is easily portable to ASIC and FPGA (Xilinx, Altera) technologies. The IP core successfully passes NIST 800-22 and AIS31 test suites and has already passed FIPS 140-2 certification.**

## General Description

All secure computer system needs good random numbers. Random numbers are used for public/private key pair generation, symmetric keys, nonce and more. Typical secure protocols like IPsec, MACsec, TLS/SSL or wireless use them during authentication/key exchange and data streaming phases.

The BA431 contains a digital true random number generator with health tests as defined in the NIST 800-90B and AIS31. The associated DRBG can support Hash_DRBG and AES_DRBG as described in the NIST 800-90A. Convenient simple FIFO and AMBA (AHB/AXI) interfaces are possible.

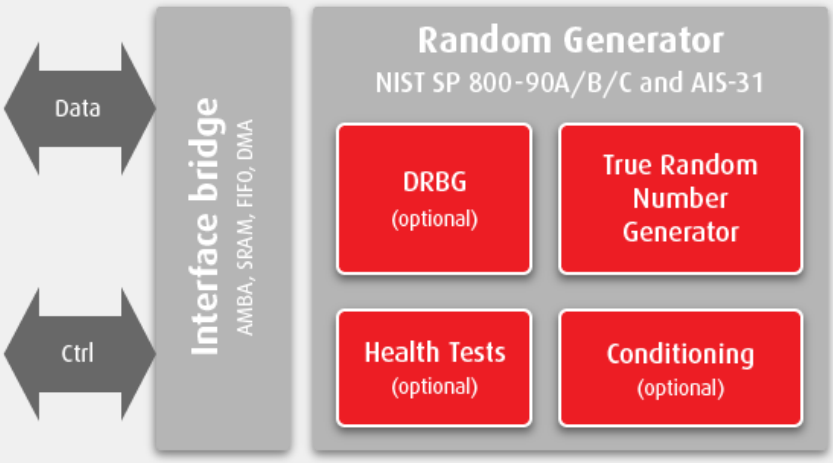


**Figure 1: TRNG/DRBG top-level description**

## Features

- True Random Generator
- Passes NIST 800-22 and AIS31 test suites
- Health tests compliant to NIST 800-90B and AIS-31
- Ready for NIST 800-90B
- Optional DRBG compliant with NIST 800-90A
- FIPS 140-2 certification
- Ready for FIPS 140-3
- Linux drivers (access from /dev/random)
- OpenSSL engine
- AMBA Interface
- Portable to FPGA and ASIC technology

## Applications

- Defense
- IPSec (VPN)
- TLS/SSL
- Automotive
- Industry 4.0
- Wearable devices
- Embedded Security

# Random Number Generator IP core

BA431 Product sheet

BarcoSilex

## 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". The Deterministic Random Bit Generator (DRBG) is also supported in software via our engine for OpenSSL. 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 is easy to port it to any technology (all ASIC nodes, Altera and Xilinx FPGA families). The random generator has been used in multiple ASIC and FPGA designs. Products from our customers have also passed FIPS 140-2 certification.

## Deliverables

- Netlist or RTL
- Scripts for implementations
- Self-checking test-bench based on FIPS vectors
- Documentation (datasheet, integration guide…)

## More Cryptography IP cores

- **BA450** Cryptographic Co-processor with Linux OS drivers for IPsec, TLS/SSL protocol
- **BA414E-PK** Public Key IP core (RSA/ECC/ECDSA/ECDH and more).
- **BA413-HASH** SHA-1/SHA-2/HMAC/MD5
- **BA412-3DES** DES/3DES
- **BA411E-FLEX** AES core for low/medium throughput and multiple cipher modes.
- **BA411E-CCM** AES core with CCM mode (Counter with CBC-MAC).
- **BA411E-XTS** AES-XTS for multi-Gbps applications.
- **BA415** AES-GCM/CTR High Throughput core (up to 100 Gb/s)

## About Barco Silex

Barco Silex is an electronic design house (ASICs, FPGAs, DSP, boards, embedded SW) specialized in video compression, security and memory controllers. Barco Silex offers the best guarantee for continuous support throughout the complete lifecycle of products.

## For more information, please contact us.

**Barco Silex SA**
Rue du Bosquet, 7
1348 Louvain-la-Neuve
Belgium

**Website** www.barco-silex.com
**Email** barco-silex@barco.com
**Phone** +32 (0) 10 454 904