INSTITUTE VLATACOM

vTRNG

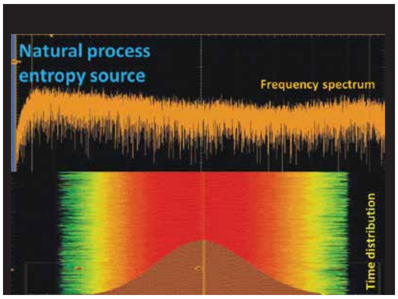
Vlatacom True Random Number Generator

Product Description

Vlatacom True Random Number Generator (vTRNG) is a natural process based long binary random sequence generator. Each produced sequence is unique. In order to prevent device misuse, prior to being stored into device's tamper-proof memory, the sequence is encrypted. The sequence randomness is tested by a bundle of statistical tests. If the sequence randomness is satisfied, it is digitally signed by the device, so its origin and quality are guaranteed. The device is equipped with an Ethernet interface and it communicates with its clients via an IP based network. Special communication protocols enable easy establishment or redundant topologies of multiple vTRNG devices.

Key Features

- Natural process based entropy source with built in entropy quality checking system
- High speed random number generation
- Satisfies the highest level of NIST 800-90A/B/C recommendation for random number generator
- Random sequence encryption by AES256 algorithm prior to storage
- Built in statistical tests according to NIST SP800-22
- Digital signing of generated sequence using built in secure access module (SAM) according to FIPS PUB 186-3
- Used for cryptographic key generation according to NIST SP800-56, SP800-133, SP800-131A and other standards.
- Proprietary secure communication protocol over Ethernet/IP networks
- Compatible with Vlatacom National Crypto Center - NCC concept

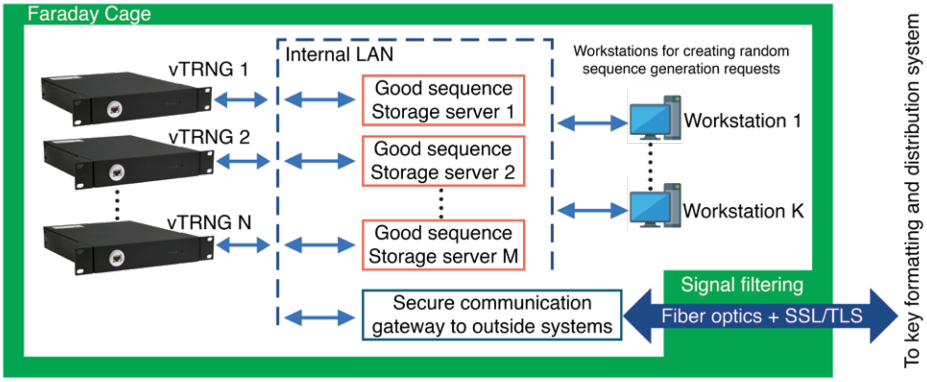


Market

The primary application of the long binary random sequence produced by vTRNG is generating cryptographic keys for both symmetrical and asymmetrical encryption algorithms. The other applications are: simulation, optimization or random marking of any kind of items (e.g. documents, banknotes, products etc.). Thus, the primary users of vTRNG are government institutions, military, police, banks, research institutions, etc.

Use Case

Since encryption quality predominantly depends on the randomness and secrecy of the used encryption keys, a typical use case for vTRNG is to establish a subsystem for state level cryptographic key generation. This is one very important component of Vlatacom's concept, the National Crypto Center. For this purpose, specially designed system architecture that gives maximal redundancy is used. In the EMC secure environment of Faraday cage: vTRNG, M good sequence storage servers, and K request workstations are installed. Generated sequences are transmitted to the external system (key formatting and distribution system) by using encrypted tunnels via a secure communication gateway that isolates the internal LAN from the outside world.


Faraday Cage
Internal LAN
Workstations for creating random sequence generation requests
vTRNG 1
vTRNG 2
vTRNG N
Good sequence Storage server 1
Good sequence Storage server 2
Good sequence Storage server M
Workstation 1
Workstation K
Signal filtering
Secure communication gateway to outside systems
Fiber optics + SSL/TLS
To key formatting and distribution system

Benefits

- Generates unique true random binary sequences
- Sequence encryption, digital signing and tamper proof case prevents any kind of device misuse
- IP based communication interface enables easy integration in any ICT system
- Redundant architecture capability gives high system availability

INSTITUTE VLATACOM

Address:
Vlatacom institute d.o.o.
Milutina Milankovića 5
11070 Belgrade, Serbia

tel: +381 11 377 11 00
fax: +381 11 377 11 99
info@vlatacom.com
www.vlatacom.com