Redefining Security

Quantis Appliance 2.0

Quantum Random Number Generator for Security Applications and Online Gaming

The Quantis Appliance distributes true and unpredictable randomness to networking and security applications and systems, for bullet-proof protection of sensitive data, servers, virtual machines and private networks. It also ensures server random pools always have true entropy and augment the entropy of random number generators in security systems such as Hardware Security Modules (HSMs) or central key management servers. Other applications include simulations or modelling.

The Quantis Appliance also helps the gaming industry to move from a dedicated to a centralized random number generation architecture, functioning as the central node of a distributed network of randomness. This allows higher flexibility, easier maintenance, better protection against any kind of physical tampering, and higher ROI.

Autonomous and non-intrusive, the Quantis Appliance seamlessly integrates into any type of networks and distributed environments. It securely delivers quantum randomness to multiple applications in parallel using standard REST API over https. It was specifically designed to meet the requirements of high availability environments with a robust FIPS-compliant chassis, redundant power supplies and hot-swap redundant fans.

Applications

- Data integrity and confidentiality
- PKI and certificate management
- User and system authentication
- Mobile subscribers authentication
- Security of virtual machines, servers, gateways and remote desktops
- Financial transactions and blockchain
- Online Gaming / Random drawings
- Randomness-as-a-service (RaaS)
- Virtual Private Networks
- Simulations and modelling

100% Trust

Only Quantum RNGs are intrinsically random and provably unpredictable. The Quantis QRNG family embeds elementary components that can be easily monitored to detect any failure or attacks. Environmental perturbations can be ruled out by simple health checks, guaranteeing the QRNG always produce high quality entropy.

WHY QUANTUM RANDOM NUMBER GENERATION?

The security of digital systems lies in the quality of the crypto algorithms and the full-entropy random numbers used to generate encryption keys, tokens or authentication certificates.

Most commonly used crypto algorithms today are standardised and open for public review. The entire foundation of security crumbles if the crypto keys used by these algorithms are not truly random and unpredictable. In other words, anything less than true entropy introduces a vulnerability.

Unfortunately, many crypto keys today are generated by Pseudo Random Number Generators (PRNGs) software that rely on deterministic algorithms and initial random seed that the computer compiles from an external source of entropy, such as the movements of the mouse, disc interrupts, or other effects. However, in many cases, especially in isolated data centers or networks, such external entropy is limited and therefore the numbers generated are not truly random.

True randomness can only be based on physical phenomena. Unlike Quantum Random Number Generators (QRNGs), random generators based on classical physics (TRNGs) are black boxes where classical physical processes run in an uncontrolled and chaotic manner. It is therefore impossible to guarantee that an attacker could not manipulate and force a classical TRNG behaviour. The only way to produce true and unbreakable randomness is by understanding and validating the physical process by which that randomness was produced.

Quantum Random Number generators (QRNGs) rely on quantum processes that are intrinsically random while well understood and can be clearly modelized and controlled to produce the highest entropy from the first bit. The Quantis Appliance exploits elementary quantum optic processes that are fundamentally probabilistic to produce true randomness.

Thanks to syslog alerts on key parameters, the Quantis Appliance can be securely managed remotely to ensure it provides true and unpredictable randomness.

TRUSTED

Simplicity is the ally of security and this is the strength of the Quantis Appliance. It relies on elementary components that can be easily controlled and monitored to ensure the random bits generated are always unpredictable.

Quantis QRNG products have been certified by many leading agencies worldwide. IDQ follows best practices and continually performs quality and security testing on its Quantis quantum random number generation products, in line with the recommendations from the most demanding standard institutions worldwide. All IDQ QRNG products pass NIST SP800-90B, SP800-22 and DieHarder tests.

SIMPLE AND PERFORMANT

The Quantis Appliance delivers quantum randomness using standard REST API over https, with a random post-processed bit rate of up to 55 Mbps. It is able to serve 8'000 requests of 256-bit keys per second from multiple threads in parallel. The system architecture has been specifically developed with parallelizable processes that allow to minimize latency and offer the best performance without compromising security, even at peak times. The Quantis Appliance can also be put in streaming mode where it delivers random bits on the fly.

The Quantis Appliance presents a simple CLI for resetting passwords and SSL certificates, and configuring network parameters. It also features a built-in web-based application for displaying system information and performances and retrieve random data files.

Easy Integration

The Quantis Appliance 2.0 seamlessly integrates into any type of networks and distributed environments and securely provide true randomness through standard REST API to multiple applications in parallel.

RELIABLE AND SECURE HARDWARE

The Quantis Appliance was specifically designed to meet the requirements of high availability environments with a robust FIPS/NEBS compliant chassis, redundant power supplies and hot-swap redundant fans. The watchdog control guarantees low maintenance efforts, ensuring an automatic restart of the Quantis Appliance if any error or malfunction occurs. Syslog alerts are generated in case of failure of the power supplies, CPU and RAMs, and the entropy source

Remote access to the appliance is possible only from allowed IP addresses and authorized users with password. SSL certificates are configurable by the admin user only.

ENTROPY FEEDER FOR LINUX AND OTHER APPLICATIONS

The Linux entropy pool is notoriously bad as it has little access to external entropy sources apart from disc interrupts and other fluctuations. By installing a daemon on the Linux host, the Quantis Appliance monitors the kernel entropy pool and feeds entropy into the pool e.g for establishing secure SSL connections. As this is done at Linux entropy pool's level, the FIPS or other security certifications of the crypto stack are retained.

Additionally, a custom-developed tool is available which enables the direct seeding of leading security systems, such as Hardware Security modules (HSMs). The user configures the Quantis Appliance to deliver a chosen rate of random numbers to the HSM, which are then mixed with the internal HSM entropy source to improve randomness and trust in the crypto functions performed by the HSM.

Key benefits

Providing true randomness and enhancing security in datacenters

- Quantum source of full entropy, intrinsically random
- True randomness from the first bit
- Provably unpredictable entropy source
- Multi-threading up to 8’000 requests/s
- Live status verification & health check output
- Seamless integration in any network or security solution
- Standard REST interface over HTTPs
- FIPS-compliant appliance designed for high availability

ID Quantique

Rue Eugène-Marziano 25
1227 Geneva, Switzerland

T +41 22 301 83 71
F +41 22 301 83 79
E info@idquantique.com

www.idquantique.com

ID Quantique (IDQ) is the world leader in quantum-safe security solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally.

IDQ also commercializes a quantum random number generator, which is the reference in the gaming and security industries.

Additionally, IDQ is a leading provider of optical instrumentation products; most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.

Quantis Appliance 2.0 at a glance

Features	Details
PERFORMANCE	
Quantum entropy source	232Mbps ± 1%
Random post-processed bit rate	55Mbps
Number of requests supported (256-bit keys)	8'000 requests/sec
RANDOMNESS CERTIFICATIONS	
NIST SP800-22 Test Suite Compliance	✓
PHYSICAL INTERFACES & PROTOCOLS	
Entropy output	RJ-45 REST API over HTTPS (TLS)
Management interface	RS-232
ADMINISTRATION AND MANAGEMENT	
Command Line Interface (SSH)	✓
Built-in webserver	System info & performances Manual random file retrieval
Secured User Access Management	✓
Syslog alerting	✓
HIGH AVAILABILITY MECHANISMS	
Watchdog	✓
Keep Alive	✓
Live Health Check	✓
PHYSICAL CHARACTERISTICS	
Dimensions	438 x 541.8 x 44.4mm
	17.2 x 21.3 x 1.75inches
Mounting	20'' fixed rail standard
Gross weight (w/ PSU & Rail)	11kg (lbs: 25.3)
Power supply	300W 1+1 redundant power supply 80 - AC INPUT: 100~240V, 50-60Hz, 5-3A - DC 36~72V input power module available
Power consumption	60W (typical)
System cooling	3 x 40 x 56mm hot swap fans
ENVIRONMENTAL	
Operating Temperature	0°C to 35°C
Storage Temperature	-10°C to 60°C
Storage & operating humidity	5-95% non-condensing
Humidity (non-operating)	5-95% non-condensing
LINUX ENTROPY INJECTION OPTION	
Operating systems supported	Ubuntu 16 & 18 CentOS 6 & 7
OTHER APPLICATIONS	
Scaling	✓
HSM Entropy Feeder	More info on request

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.