Redefining Security

Quantis Appliance

Quantum Random Number Generator for Networked and Security Applications

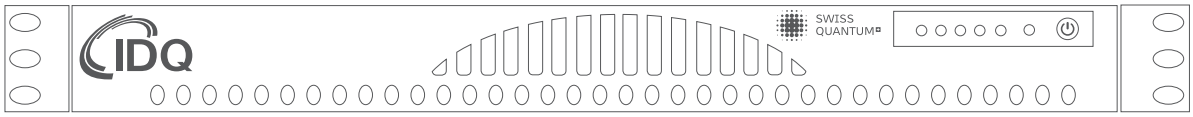
ID Quantique provides highly secure quantum key generation based on the Quantis Quantum Random Number Generator (QRNG) product family. The company is also a leader in high-performance quantum-safe network encryption solutions for the protection of data in transit, using state-of-the-art algorithms and quantum key distribution.

The Quantis Appliance is a network-attached device, which securely generates and delivers high-quality randomness for security and cryptographic applications in enterprise, government, academic, gaming and cloud environments.

High quality randomness is at the foundation of all cryptography. Modern cryptographic systems are based on mathematical models (algorithms). Every algorithm works in a predefined manner according to a set of mathematical formulas and transformations.

What is unique to each cryptosystem is its key material. Hence, in order to ensure security, all crypto keys need to be properly generated (unique and truly random). Moreover such cryptographic systems need to be continuously fed with true randomness in order to ensure the integrity of the security systems they protect.

The random numbers provided by the Quantis Appliance can be used for different applications: to generate high-quality cryptographic keys for encryption or authentication; to seed deterministic PRNGs; or to supply commercial HSMs with additional randomness and true entropy.



Key Markets

- Financial Services Companies
- Data Centers
- Cloud Services Providers
- Telecommunications

Key Benefits

- Trusted and certified source of quantum randomness
- State-of-the-art Swiss Quantum Random Number Generation
- Designed to support multiple operating platforms
- Easy management of application environments

Quantis Appliance

Quantum Random Number Generator

The Quantis Appliance is a network-attached device, which securely generates and delivers high quality random numbers for security and cryptographic applications in enterprise, government, academic, gaming and cloud environments.

WHY QUANTUM RANDOM NUMBER GENERATION?

The foundation of modern digital security systems lies in the quality of the crypto algorithms and encryption keys. Most commonly used crypto algorithms today are standardised and open for public review. In accordance with the Kerckhoff principle, a crypto system must be secure if everything about it is known, except the encryption key itself. Therefore the entire foundation of security crumbles if the numbers that have been generated to create a key are not unique or sufficiently random. In other words, anything less than true randomness (or entropy) introduces a vulnerability.

Unfortunately, many keys today are currently created by pseudo random number generators (PRNGs) meaning a computer program supplies the randomness for generating keys. It is no secret that computer programs are deterministic, and therefore predictable. This means that, in most cases, the computer tries to draw in entropy from an external source, such 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.

A true random number is a number generated by a process whose outcome is unpredictable, and which cannot be subsequently reliably reproduced. The only way to produce true randomness is by understanding and validating the physical process by which that randomness was produced. In other words, randomness can only be based on physical phenomena. Since quantum physics is intrinsically random, it is logical to use it as a source of true randomness.

Quantum Random Number Generators (QRNGs) have the advantage over conventional randomness sources of being invulnerable to environmental perturbations and of allowing live status verification. The operation of the Quantis QRNG is continuously monitored and if a failure is detected the random bit stream is immediately disabled. In addition, unlike PRNGs which need to accumulate external entropy, the Quantis Appliance provides full entropy (randomness) instantaneously from the very first bit.

PERFORMANCE

Operating at a maximum throughput of 16 Mbps, the Quantis Appliance is able to serve multiple clients in parallel seamlessly with random data ranging from 1 byte to several Gigabytes. The system architecture has been specifically developed with parallelisable processes that allow to minimise latency and to offer the best performance without compromising security. Nevertheless the design of the Quantis Appliance guarantees that even if the system is overloaded at peak times, it delivers the best quality randomness with a minimum waiting period. For requests of huge random data the Quantis Appliance can also be put in streaming mode where it starts to deliver the generated random bits on the fly.

RESILIENCE

The Quantis Appliance was specifically designed to meet the requirements of high availability environments. It can be inserted in, or removed from, an operating network with no impact on any other appliance (servers, Hardware Security Modules, etc). Using an Ethernet port, the Quantis Appliance is a distributed device that can provide several systems with randomness. It is autonomous and integrates seamlessly into different types of networks. The Quantis Appliance provides high quality randomness to any number of connected devices.

ON-DEMAND VALUE ADDED MODULES

The Quantis Appliance serves as a hardware source of trust for cloud or distributed environments, with both Linux and Windows operating systems. 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 connection. As this is done on the level of the Linux entropy pool, the FIPS or other security certifications of the crypto stack are retained.

Quantis Appliance

100% Trust — True randomness with certified internal QRNG

Quantis has been certified by leading commercial and government entities, from the Swiss Federal Office of Metrology (METAS certificate), to the French ANSSI in accordance with the German BSI's AIS31 validation criteria.

Additionally, a custom-developed tool is available which enables the direct seeding of leading Hardware Security modules (HSMs) without the need for an external server. 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.

The Quantis Appliance provides secure keys for Virtual Machines (VMs), Virtual Private Networks (VPNs), HSMs and remote desktops. It is also used in Randomness-as-a-service (RaaS) or Security (SaaS) environments.

EASY MANAGEMENT

The Quantis Appliance provides an intuitive web-based application. Configuration management is done through CLI (Command Line Interface).

For troubleshooting, the Quantis Appliance supports syslog which provides a correlated view on the log data generated by different system components. Data about the status, events and diagnostics of the device are stored. The watchdog control guarantees low maintenance, ensuring an automatic reboot of the Quantis Appliance if any error or malfunction occurs.

TRUSTED AND CERTIFIED

Simplicity is the ally of security and this is the strength of the Quantis Appliance. As the quantum mechanical processes underlying the QRNG are well understood and characterised, and since the quantum optics process itself is transparent, it is relatively simple to achieve otherwise stringent certifications of the Quantis QRNG products. Quantis has been certified by leading commercial and government entities, from the Swiss Federal Office of Metrology (METAS certificate), to the French ANSSI in accordance with the German BSI's AIS31 validation criteria.

Why the Quantis Appliance?

True Quantum Randomness

- Certified Quantum Random Number Generator (QRNG)
- High performance and easy configuration
- Entropy source up to 16 Mbps

For Networked Applications

- High quality random numbers for security and cryptographic applications
- Transparent supply of proven randomness into applications
- Swiss certified randomness source for HSMs to improve trust and security

Quantis Appliance at a glance

Features	Details
RANDOM BIT RATE	
Quantis Appliance-4M	4 Mbit/s
Quantis Appliance-16M	16 Mbit/s
INTERFACES	
Data Interface	1000BaseT
Configuration Interface	RS-232
Protocol	REST API, JSON, HTTP/HTTPS (TLS)
API	Swagger UI
ADMINISTRATION / MONITORING / TROUBLESHOOTING	
Command Line Interface on Serial port	✓
Syslog	✓
Inbound Admin/Monitoring	✓
Web-app based interface	✓
HIGH AVAILABILITY MECHANISMS	
Watchdog	✓
Keep Alive	✓
Live Health Check	✓
ADDITIONAL SW FEATURES (EVOLVING)	
Linux Entropy Injection	✓
HSM Entropy Feeder	More info on request
Scaling	✓
OPERATING SYSTEM	
Windows	✓
Linux	✓
Any operating system	Through REST API formatted in JSON over HTTTP/HTTPS.
RANDOMNESS CERTIFICATIONS	
NIST	✓
METAS	✓
AIS31	More info on request
CTL	✓
PHYSICAL CHARACTERISTICS	
Dimensions	19” 1U (427x43x356mm WxHxD)
Power Consumption	50 W (100-240 V; AC)
ENVIRONMENTAL	
Operating Temperature	10°C to 35°C
Non-Operating Temperature	0°C to 70°C
Humidity (operating)	8-90% non-condensing
Humidity (non-operating)	5-95% non-condensing

ID Quantique

Chemin de la Marbrerie 3,
1227 Carouge/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.