IDQ
FROM VISION TO TECHNOLOGY

SWISS QUANTUM

REDEFINING RANDOMNESS

QUANTIS APPLIANCE

TRUE QUANTUM RANDOMNESS FOR NETWORKED & SECURITY APPLICATIONS

The Quantis Appliance

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, gaming and cloud environments. The Quantis Appliance is designed for environments, where high availability is necessary. It can be inserted in, or removed from, an operating network with no impact on any other appliance (servers, Hardware Security Modules (HSMs), etc....).

The random numbers generated by the Quantis Appliance are used for different applications: to generate high-quality cryptographic keys for encryption or authentication; to seed deterministic PRNGs and provide additional randomness for commercial HSMs; or to provide entropy for online gaming and mathematical simulations.

The Quantis Appliance serves as a hardware source of trust for cloud or distributed environments, with both Linux and Windows operating systems. It 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 as a Service (SaaS) environments.

MAIN FEATURES

- True quantum randomness, with certified internal QRNG
- High bit rate up to 16 Mbits/s
- 1000BaseT (Ethernet 1 Gbps) interface
- Hot pluggable and swappable
- Runtime health check and automatic reboot in case of anomalies
- Easy integration in applications and systems
- Rackable system: standard 19" 1U

APPLICATIONS

- Cryptographic key generation for cloud and network environments
- Seeding of deterministic PRNGs or commercial HSMs
- Entropy generation for servers in data centers
- Randomness as-a-Service
- Online gaming services

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge / Geneva
Switzerland
T: +41 22 301 83 71
F: +41 22 301 83 79
info@idquantique.com
www.idquantique.com

REDEFINING RANDOMNESS

QUANTIS APPLIANCE

THE NEED FOR RANDOMNESS

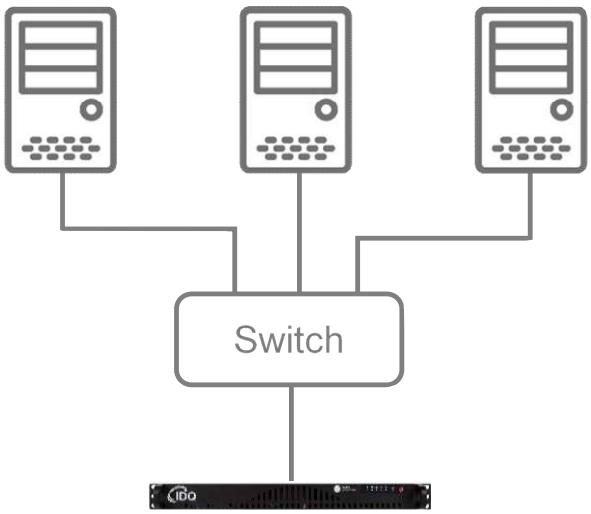
Although random numbers are required in many applications, their generation is often overlooked. Low quality random numbers may represent a serious attack vector. The Quantis Appliance is based on IDQ's industry-leading Quantis Quantum Random Number Generator (QRNG), which harnesses elementary quantum optical processes as a source of entropy (entropy is a measure of disorder; a physical source of entropy is needed in order to generate random numbers) and provides true randomness.

Pseudo Random Number Generators
In contrast to the Quantis, software-based Random Number Generators (RNGs), also known as Pseudo RNGs (PRNGs), are deterministic. They do not generate entropy. Therefore, for most applications, they need to be seeded with an entropy source, which brings back in full circle to the generation of truly random numbers.

True Random Number Generators
True Random Number Generators (TRNGs) have to be based on some physical phenomenon. Conventional TRNGs, based on classical physics, rely on complex chaotic systems to generate entropy. The main drawbacks of such systems are their possible sensitivity to environmental conditions, and the fact that the entropy generation is hidden in a complex structure. In contrast, QRNGs are invulnerable to environmental perturbations. Entropy generation derives directly from the principles of quantum mechanics. Quantum processes provide full, instantaneous and inexhaustible entropy.

POSSIBLE SCENARIOS

1. **Quantis Appliance with multiple servers**



The Quantis Appliance with multiple servers

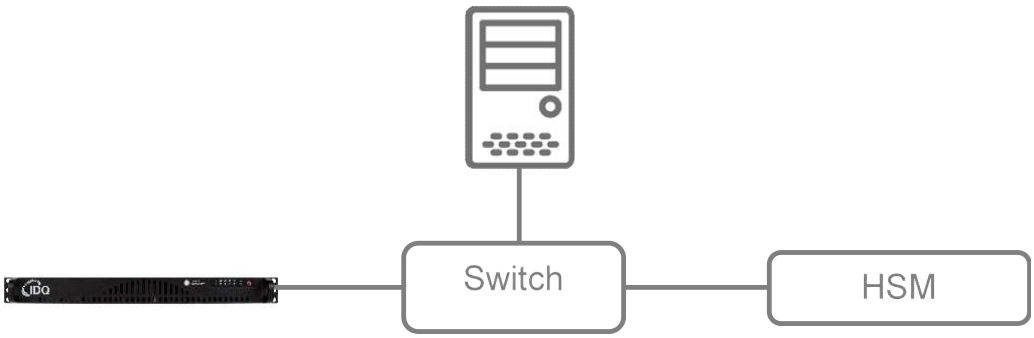
The Quantis Appliance is connected to multiple servers through a switch. It is hot pluggable and swappable. The random numbers obtained by the servers can be used in any application.

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge / Geneva
Switzerland
T: +41 22 301 83 71
F: +41 22 301 83 79
info@idquantique.com
www.idquantique.com

REDEFINING RANDOMNESS

QUANTIS APPLIANCE

2. **Quantis Appliance seeding an HSM**



The Quantis Appliance seeding random numbers to an HSM through a server

The different elements, server, HSM and the Quantis Appliance are integrated in a LAN. The server organizes the communication to the devices, and orchestrates the distribution of random numbers to the HSM. The Quantis Appliance is hot pluggable and swappable, ensuring seamless integration, even within an operating network.

3. **Quantis Appliance directly seeding a Safenet Network HSM**

The Quantis Appliance directly seeding random numbers to a Safenet Network HSM

A proprietary tool was developed by ID Quantique to enable direct seeding of the Safenet Network HSMs (Luna SA 4 and Luna SA 5), without the need for an external server. The user configures the Quantis Appliance to deliver a chosen rate of random numbers to the HSM. Tools for other types and other brands of HSMs will be added at a later stage. The Quantis Appliance is hot pluggable and swappable, ensuring seamless integration with an operating HSM.

QUANTIS CERTIFICATIONS

- Certified by Swiss National Metrology Laboratory (METAS)
- Certified by numerous governments & gaming houses
- Passes NIST & DIEHARD randomness tests

INTEGRATION

- ID Quantique offers an integration service or an SDK for your own integration. With ID Quantique integration service, our SW engineers will perform the integration of the Quantis Appliance into your network.
  Contact factory for details.

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge / Geneva
Switzerland
T: +41 22 301 83 71
F: +41 22 301 83 79
info@idquantique.com
www.idquantique.com

REDEFINING RANDOMNESS

QUANTIS APPLIANCE

TECHNICAL SPECIFICATIONS

Random bit rate	4 Mbit/s ± 10% (Quantis Appliance-4M) 16 Mbit/s ± 10% (Quantis Appliance-16M)
Dimensions	19" 1U (427x43x356mm WxHxD)
Data interface	1000BaseT
Configuration interface	RS-232
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
Power consumption	200-300 W (100-240 V; AC)
Tamper evident casing	

SYSTEM PROTECTION

- Internal protection against power interruptions
- Watchdog reboots if service hangs up
- Live status verification of embedded QRNG

SOFTWARE & PROGRAMMING

Protocol	XML over HTTP over TLS over TCP/IP
Configuration	CLI via RS-232
Programming	Programmable with any language and any operating system. Provided with a Software Development Kit (SDK) for “C” with Linux OS, and an example SW in “C”

RELATED PRODUCTS

Quantum Key Factory	The Quantis Appliance can be used as an entropy seed for the Quantum Key Factory, a solution platform for creating cryptographically secure digital keys/tokens.

OPTIONS AND ORDERING INFORMATION

Quantis Appliance-4M	Quantis Appliance; random bit rate: 4 Mb/s
Quantis Appliance-16M	Quantis Appliance; random bit rate: 16 Mb/s

Quantis Appliance v1.0- Specifications as of February 2016

Partners

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge / Geneva
Switzerland
T: +41 22 301 83 71
F: +41 22 301 83 79
info@idquantique.com
www.idquantique.com