Quintessence Labs

qStream™

100 | 200

Strengthen your data protection using high-speed true random number generation

- True random numbers for the strongest encryption
- Supports KMIP for compatibility with a wide array of security platforms
- Available as an appliance or a PCIe card

Overview

Random numbers are fundamental to data security. They are used to generate encryption keys and other parameters at the heart of data protection. Random numbers are at the core of most security applications, as well as numerical simulations, random sampling, and gaming.

It is important that the output from random number generators is both unpredictable and has a high enough throughput for commercial use. QuintessenceLabs' qStream™ quantum random number generator (QRNG) uses groundbreaking quantum technology to deliver random numbers with full entropy at 1 Gbit/sec, providing both the randomness and the speed required.

The Quality of Random Numbers

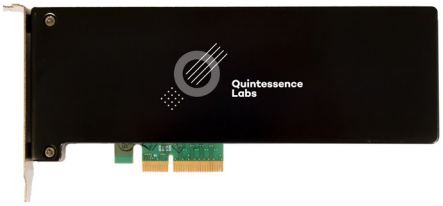
When it comes to data security, the quality of random numbers has a big impact on the success of encryption and overall security. Most applications use pseudo-random numbers generated by algorithms from a randomization "seed." These deterministic methods are not always safe: pseudo-random can be of low-quality and reduce the strength of encryption, increasing security risks.

Conversely, true random numbers — also known as "full entropy" random numbers — are perfectly unpredictable and deliver cryptographic keys of the highest quality, enabling strong encryption. They have proven to be extremely difficult to generate, especially at the high throughputs needed for commercial use. The qStream QRNG has solved that problem, using quantum innovation to deliver truly random numbers at very high speeds.

qStream QRNG Capabilities

The qStream QRNG provides true random numbers to applications, servers, and key management systems to support data protection, numerical simulations, gaming and other uses.

The qStream QRNG delivers random numbers through the industry-standard OASIS Key Management Interoperability Protocol (KMIP), enabling interoperability with any conformant key management server, such as our Trusted Security Foundation® (TSF®) key and policy manager. Raw entropy, conditioned entropy and random numbers can also be delivered to clients over a standard TCP/IP network connection, or via mutually authenticated TLS at up to 1 Gbit/sec.



qStream QRNG Deployment

Integrating the qStream QRNG appliance into your existing security infrastructure is as simple as installing any other appliance or device in your network.

The qStream™ 100 quantum random number generator (QRNG) is a PCIe Gen 2 card that adds true random number generation to existing appliances. It delivers the same full entropy random numbers sourced from two integrated 8 Gbit/sec quantum entropy sources. (See reverse side for full comparison between qStream 100 and 200 products.)

The qStream™ 200 quantum random number generator (QRNG) supports hot-swappable power supplies, fans, and hard drives for straightforward maintenance when needed. Management is performed through a web-based (HTTPS) interface, TLS-protected API calls, or via SSH command line.

qStream QRNG products can also directly integrate with the QuintessenceLabs' TSF key and policy manager. The TSF key and policy manager is the preferred choice for management of qStream's quantum random number generation, and like qStream applications, supports KMIP and other standards.

SPECIFICATIONS

qStream™

100 | 200

High-speed, full entropy QRNG appliance

	qStream 100	qStream 200
Configuration & Dimensions	PCIe Gen 2 card module • Width: 6.43 cm (2.53") • Length: 16.94 cm (6.67") • Height (Thickness): 1.35 cm (0.53") • Weight: 297.7 g (0.66 lbs.)	Rackmount Appliance • Dimensions: 1RU: H: 4.28 cm (1.69"), W: 48.20 cm (18.98") D: 80.85 cm (31.83") • Weight: 22 kgs (48.50 lbs) • Support for running multiple Virtual Machines (VMs)
Performance	• 8Gbit/sec quantum entropy source • Outputs: up to 1 Gbit/sec conditioned entropy (QRNG) up to 1 Gbit/sec unconditioned entropy	
	N/A	Supports thousands of end-client systems and up to 8,000 key requests per minute per node in TSF key and policy manager implementations
Operations	• Raw and conditioned entropy output (via DMA bus)	• Raw and conditioned entropy output (via TCP, TLS)
	N/A	• Hardened OS • Granular, auditable access control • Attended or unattended startup • Logging of events and audits
Standards & Interoperability	• OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4/2.0 with extensions for secure Random Object management • Meets all requirements of NIST SP 800-90A, 90B and 90C (draft) standards for Non-Deterministic Random Bit Generators • Satisfies NIST SP 800-22 (NIST STS) and Dieharder tests • Supports PKCS#11 over KMIP	
Administration & Management	N/A	• Web (HTTPS) or command-line (SSH) management interfaces • Purpose-built QRE secure operating system • Delivered with qClient™ 100 • Support for 10 Gbit/sec Ethernet
Power Consumption	12.78 Watts	• 100–240 V AC, autoranging, 50/60 Hz • 1RU Power Supply: Dual, redundant, hot-swappable, 550W

Quintessence Labs

AUSTRALIA
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 1620