Quintessence Labs

# qStream™

## 100A | 100P

Strengthen Your Data Protection Using
High-Speed True Random Number Generation

- Truly 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. qStream uses groundbreaking quantum technology to deliver random numbers with 100 percent entropy at 1 Gbit/s, providing both the randomness and the speed required.

### The Quality of Random Numbers

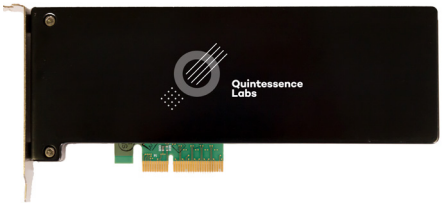
When it comes to data security, the quality of random numbers has a big impact on the success of encryption and overall security. Most applications use pseudo-random numbers generated by algorithms that build from a randomization "seed." These deterministic methods are not always safe: pseudo-random 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 been extremely difficult to generate, especially at the high throughputs needed for commercial use. qStream has solved that problem, using quantum innovation to deliver truly random numbers at very high speeds.

### qStream Capabilities

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

qStream delivers random numbers through the industry-standard OASIS Key Management Interoperability Protocol (KMIP), enabling interoperability with any conformant key management server, such as qCrypt from QuintessenceLabs. 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/s.




### qStream Deployment

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

The qStream 100A rackmount appliance 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.

The qStream 100P 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/s quantum entropy sources. (See reverse side for full comparison between qStream 100A and 100P products.)

qStream products can also directly integrate with qCrypt, QuintessenceLabs' encryption key and policy manager. qCrypt is the preferred choice for management of qStream's true random number generation, and like qStream, supports KMIP and other standards.

SPECIFICATIONS

# qStream™

## 100A | 100P

| | qStream 100A | qStream 100P |
|---|---|---|
| **Configuration** | Rackmount appliance | PCIe Gen 2 card module |
| **Performance** | • 8Gbit/s quantum entropy source<br>• **Outputs:**<br>1Gbit/s conditioned entropy<br>1Gbit/s unconditioned entropy<br>1Gbit/s true random (TRNG) | |
| | Supports thousands of end-client systems and up to eight thousand key requests per minute per node in qCrypt/TSF implementations | N/A |
| **Operations** | • Raw and conditioned entropy output (via TCP, TLS) | • Raw and conditioned entropy output (via DMA bus) |
| | • Supports PKCS#11 via KMIP protocols<br>• Hardened OS<br>• Granular, auditable access control<br>• Attended or unattended startup<br>• Logging of events and audits; user reports and management | N/A |
| **Standards & Interoperability** | • **OASIS KMIP:** Conformant with standards 1.0, 1.1, 1.2, 1.3, 1.4, with extensions for secure Random Object management<br>• Meets all requirements of NIST SP-800-90A, B and C (draft) standards for Non-Deterministic Random Bit Generators | |
| **Administration & Management** | • Web (HTTPS) or command-line (SSH) management interfaces<br>• Purpose-built qRE secure operating system<br>• Includes qClient SDK | N/A |
| **Dimensions** | • **Height:** (2U) 3.5”/8.8cm<br>(1U) 1.75”/4.4cm<br>• **Depth:** (2U) 27.5”/69.85cm<br>(1U) 25”/63.5cm | • **Width:** 2.53”/ 6.43cm<br>• **Length:** 6.67”/ 16.94cm<br>• **Height (Thickness):** 0.53”/ 1.35cm<br>• **Weight**: 10.5 oz. (0.65 lbs.) |
| **Power Consumption** | • 90-264 VAC, 47-63Hz input<br>• 450W power supply | 12.78 Watts |



Quintessence Labs

**AUSTRALIA**
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+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