

# qStream™

## 100A | 100P

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. qStream uses groundbreaking quantum technology to deliver random numbers with true entropy at 1 Gbit/sec, providing both the randomness and the speed required.

### The Quality of Random Numbers

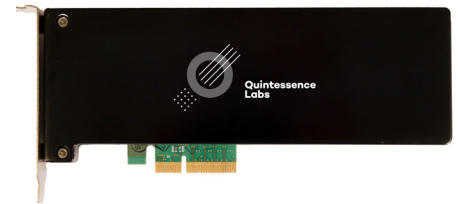
When it comes to data security, the quality of random numbers has a big impact on the success of encryption and overall security. Most applications use pseudo-random numbers generated by algorithms from a randomization “seed.” These deterministic methods are not always safe: pseudo-random can be of low-quality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



### 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/sec 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
<b>Configuration</b>	<b>Rackmount Appliance</b> <ul style="list-style-type: none"> <li>• Dimensions: 1RU: H: 4.28 cm (1.69"), W: 48.20 cm (18.98") D: 80.85 cm (31.83")</li> <li>• Weight: 22 kgs</li> <li>• Support for running multiple Virtual Machines (VMs)</li> </ul>	PCIe Gen 2 card module <ul style="list-style-type: none"> <li>• Width: 6.43 cm (2.53")</li> <li>• Length: 16.94 cm (6.67")</li> <li>• Height (Thickness): 1.35 cm (0.53")</li> <li>• Weight: 297.7 g (0.66 lbs.)</li> </ul>
<b>Performance</b>	<ul style="list-style-type: none"> <li>• 8Gbit/s quantum entropy source</li> <li>• Outputs:               <ul style="list-style-type: none"> <li>up to 1 Gbit/sec conditioned entropy (QRNG)</li> <li>up to 1 Gbit/sec unconditioned entropy</li> </ul> </li> </ul>	
	Supports thousands of end-client systems and up to eight thousand key requests per minute per node in qCrypt/TSF implementations	N/A
<b>Operations</b>	<ul style="list-style-type: none"> <li>• Raw and conditioned entropy output (via TCP, TLS)</li> </ul>	<ul style="list-style-type: none"> <li>• Raw and conditioned entropy output (via DMA bus)</li> </ul>
	<ul style="list-style-type: none"> <li>• Hardened OS</li> <li>• Granular, auditable access control</li> <li>• Attended or unattended startup</li> <li>• Logging of events and audits</li> </ul>	N/A
<b>Standards &amp; Interoperability</b>	<ul style="list-style-type: none"> <li>• OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4/2.0 with extensions for secure Random Object management</li> <li>• Meets all requirements of NIST SP 800-90A, 90B and 90C (draft) standards for Non-Deterministic Random Bit Generators</li> <li>• Satisfies NIST SP 800-22 (NIST STS) and Dieharder tests</li> <li>• Supports PKCS#11 over KMIP</li> </ul>	
<b>Administration &amp; Management</b>	<ul style="list-style-type: none"> <li>• Web (HTTPS) or command-line (SSH) management interfaces</li> <li>• Purpose-built QRE secure operating system</li> <li>• Delivered with qClient SDK</li> <li>• Support for 10 Gbit/sec Ethernet</li> </ul>	N/A
<b>Power Consumption</b>	<ul style="list-style-type: none"> <li>• 100–240 V AC, autoranging, 50/60 Hz</li> <li>• 1RU Power Supply: Dual, redundant, hot-swappable, 550W</li> </ul>	12.78 Watts