Quintessence
Labs

qRand™ Entropy Management Software

Quantum-Powered Entropy Enhancer & Entropy Broker

Ensures sufficient entropy, preventing entropy starvation

Supports mulitple entropy sources and API's

Enables Entropy as a Service (EaaS) functionality

OVERVIEW

QuintessenceLabs' qRand™ Entropy Management Software, Entropy Enhancer and Entropy Broker, are Linux software daemons that provide two distinct but collaborative entropy management functions.

When used with the QuintessenceLabs' qStream™ Quantum Random Number Generator (QRNG), the Entropy Enhancer manages entropy levels on the target platform and improves entropy quality. The Entropy Broker allows for multiple entropy sources, including the qStream QRNG, to be utilized and distributed via user-defined APIs.

ENTROPY ENHANCER

qRand Entropy Enhancer monitors entropy status on a server or computer, and when it falls below a defined lower bound, augmenting it with additional entropy addressing the problem of 'entropy starvation'.

Entropy starvation degrades performance, with applications failing to respond due to a lack of randomness for cryptographic operations. The Entropy Enhancer ensures that Linux servers have enough entropy. This is especially important for hypervisors and virtual Linux instances which are prone to suffer from entropy starvation.

ENTROPY BROKER

qRand Entropy Broker is a service that allows users to draw entropy from multiple Entropy Sources and provide it to users and end services via a range of APIs. It is possible to mix multiple Entropy Sources via a bitwise XOR operation. Additionally, each Entropy Provider supports failover functionality and buffers its Entropy Sources.

The Entropy Broker allows changes to existing Entropy Sources transparent to the end service drawing entropy: migration to an Entropy Source that uses a different API than the original, adding a fallback Entropy Source to an existing Entropy Source, adding buffering to an existing Entropy Source, and allowing the mixing of multiple Entropy Sources via bitwise XOR.

QSTREAM QRNG

Quantum Random Number Generator

qStream QRNG generates 1 Gbit/s of true random numbers providing 100% quantum entropy.

qStream is available in three form factors:

- qStream 100 PCIe Adapter with Software Development Kit (SDK) for integration into applications requiring high-quality entropy.
- qStream 200 Network Attached Appliance providing quantum entropy 'out-of-the-box', great for Entropy as a Service (EaaS) deployments.
- qStream Entropy as a Service (EaaS) is a quantum entropy service available for consumption on a subscription basis.

Entropy as a Service (EaaS) Use Case

- Entropy as a Service (EaaS) is a service providing secure quantum entropy sources to devices and applications in need of high-quality entropy.
- The qStream 200 QRNG Network Attached Appliance supported by qRand Entropy Management Software enables organizations to establish internal or external facing Entropy as a Service deployments.

SPECIFICATIONS

qRand™ Entropy Management Software

Quantum-Powered Entropy Enhancer & Entropy Broker

Key Features

- Both – Linux daemon, running as a native system service
- Both – User configurable entropy sources
- Both – Can mix entropy sources
- Enhancer – Provides random to OS entropy pool and/or user-defined device
- Broker – Provides random via user-defined network APIs

User Settings

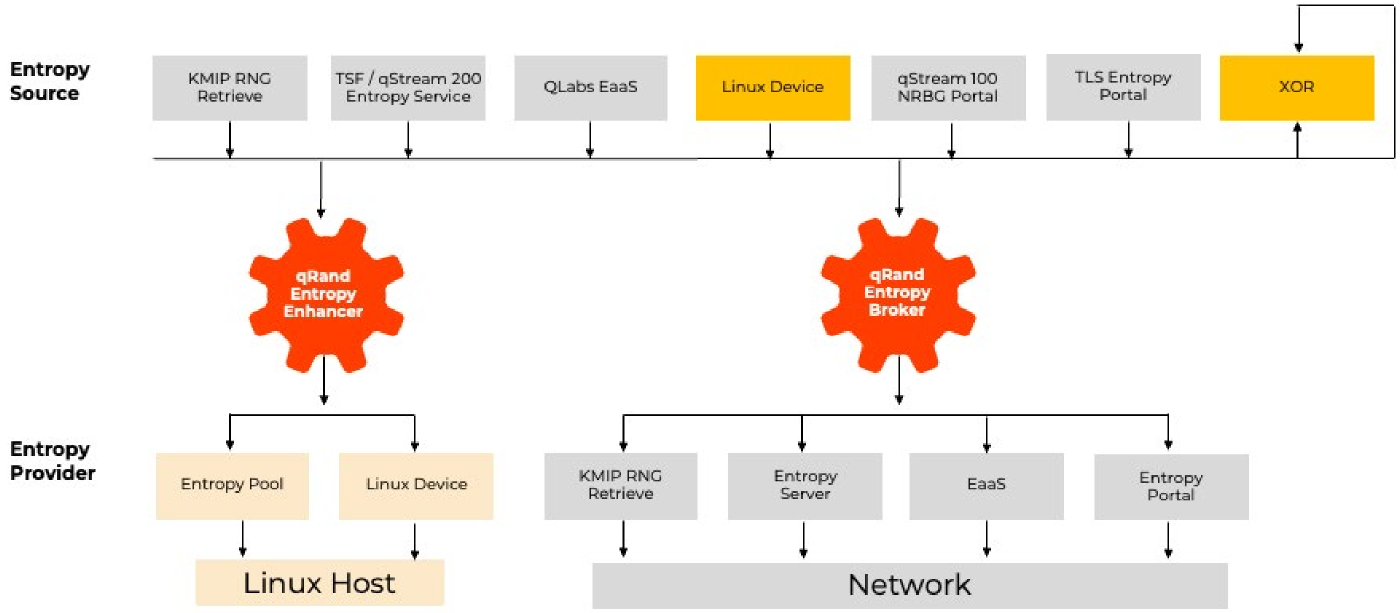
- Both – Entropy sources
- Both – Entropy provider outputs
- Both – Buffer sizes and thresholds
- Enhancer – Low OS Entropy threshold

Supported OS

- Both – Linux x86-64
- Broker – Windows x86-64

Supported Entropy Sources

- Both – KMIP RNG Retrieve
- Both – qStream/TSF Network Attached Appliance entropy service
- Both – Cloud Entropy as a Service (EaaS)
- Both – Linux device
- Both – Local qStream 100 portal
- Both – TLS entropy portal
- Both – XOR of 2 . . n entropy sources



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: 6726-00