THE
QUANTUM WORLD
CORPORATION

P.O. Box 5039, Gainesville, FL 32627,
(352) 334-7299
contact@ComScire.com

July 11, 2012

To Whom it May Concern,

ComScire® – Quantum World Corporation certifies that its QNG Model R32MU hardware true random number generator will pass any properly designed test for randomness. Furthermore, the R32MU's design makes it virtually impervious to any attempt to influence or control the random output sequence.

Every true random number generator (TRNG) requires a physical source of entropy. Entropy is in general a measure of disorder in a physical system. In terms of Information Theory, entropy can be thought of as a measure of how unpredictable the measured properties of the entropy source are. The entropy source in the QNG Model R32MU is a combination of thermal or Johnson noise and transistor noise. Eight independent, high-frequency oscillating signal sources, each including combined noise signals of the type described above, continuously operate at different frequencies between 200 and 400 MHz. The resulting noisy oscillator signals are each sent through multi-stage delay lines to produce 32 additional noisy outputs. Permutations of these additional noisy outputs are used to produce 64 sampled binary signals. The sampled binary signals are combined and resampled at an output frequency of 128 MHz. The effect of the delay lines and the many permuted binary samples is to greatly increase the rate of sampling of the entropy, that is, the unpredictability of the combined output bits.

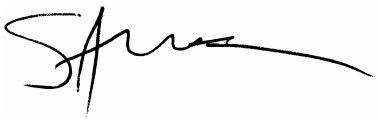
The R32MU contains three independent generators of the type described above. The statistics of each of these three generators is continuously monitored in the generator hardware. The monitoring includes 1/0 bias, 1^{st} order autocorrelation and an estimated minimum entropy. The outputs of each of the three generators is then sent through a nonlinear feedback shift register (NLFSR) whitening function to correct defects in statistical randomness. The NLFSR's do not change the total amount of entropy, but distribute it equally over the bits in the output sequences. The three corrected outputs are combined by XOR function and finally 4 of these bits (8 bits if the output rate is set to 16 Mbps) are combined in another XOR to produce each final output bit. The internal hardware monitoring requires at least two of the three generators to have an estimated entropy of at least 0.95 bits/bit. If this requirement fails, the output from the generator is halted. Output bits are also tested for entropy, and the generator will be halted if the estimated entropy falls below 0.99 bits/bit. The internal hardware testing also acts as a startup test program. At startup random data will not be output until a block of 1,048,576 bits (2^{20} bits) from at least two of the three redundant generators has produced the required minimum entropy level.

Interface software in the host computer monitors the flow of data from the generator. If the monitoring program detects a halt condition, a request for the internal statistics from the raw data streams will be automatically generated. These statistics are checked to determine if there has been an actual fault in the hardware, and if this check indicates a fault, an error message will be generated and no random data will be provided. The automatic check of the hardware may also indicate there was simply a delay caused by normal functioning in the computer's operating system, programs or other attached components. If the check shows the hardware is operating correctly, the monitoring software will restart the generator output and random data flow will resume. The internal statistical test results are accessible at any time through simple commands in the user interface.

The generator is housed in a grounded, 1/16 inch aluminum device enclosure, which prevents both monitoring of output bits and interference with the generator by electromagnetic fields. Power is provided through the USB connector and is filtered at entry into the shielded enclosure. Independent regulation of power for the generator section prevents any external effect on the random number generation by fluctuations in the power source.

The R32MU is used for cryptographic purposes as well as online gaming and other applications requiring the highest levels of security and randomness properties, and the highest speed available for any USB-connected TRNG The R32MU has been tested extensively well-known test suites such as DIEHARD and NIST 800-22. In addition, each generator is continuously tested by our QNGmeter test suite to 1000 billion bits (1Tb) or more to verify compliance with our internal specifications, which are more stringent than either DIEHARD or NIST testing reveal.

Sincerely,



Scott Wilber, President