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 R2000KU hardware true random number generator will pass any properly designed test for randomness. Furthermore, the R2000KU'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 R2000KU is a combination of thermal or Johnson noise and transistor noise. Four 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 16 additional noisy outputs. Permutations of these additional noisy outputs are used to produce 32 sampled binary signals. The sampled binary signals are combined and resampled at an output frequency of 112 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 R2000KU 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 linear feedback shift register (LFSR) whitening function to correct defects in statistical randomness. The LFSR'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 56 of these bits (112 bits if the output rate is set to 1 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 0.9 bits/bit. If this requirement fails, the output from the generator is automatically halted. Output bits are also tested for entropy, and the generator will be halted if the output 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.

Power for the generator is provided through the USB connector and is filtered at entry into the grounded, 1/16 inch aluminum device 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 R2000KU is used for cryptographic purposes as well as online gaming and other applications requiring the highest levels of security and randomness properties. The R2000KU has been tested extensively both internally and by independent companies using well-known test suites such as DIEHARD and NIST 800-22. In addition, each generator is continuously tested by our RNGmeter test suite to 100 billion bits or more to verify compliance with our internal specifications, which are more stringent than either DIEHARD or NIST testing reveal.

Sincerely,

Scott Wilber, President