

Certification for Random Number Generator and Shuffling Algorithm

1 December 2013

Cigital Ltd, a leading software security consultancy, was contracted by Rational Entertainment Enterprises Limited (REEL) to evaluate the random number generating system consisting of a hardware random number generator (RNG) and related software. Cigital also tested the shuffling algorithms and examined the resulting virtual decks to analyse the randomness and uniformity of shuffles.

1.0 Testing

Cigital obtained a sample hardware random number generator as well as software source code from REEL. Sample output was gathered from the RNG and tested under controlled conditions at Cigital Labs in Dulles, Virginia, USA. Output of the random number generator was tested using two well-known test suites: [the statistical randomness test suite](#) from the [U.S. National Institute of Standards and Technology \(NIST\)](#) and the [Dieharder v3.31.1 statistical randomness tests](#). Cigital analysts also performed manual review of the source code related to the use of the RNG and its output.

Cigital designed and carried out a method for determining whether shuffles of virtual decks of cards were unpredictable, unbiased, and statistically random. This methodology was carried out for virtual decks of size 52 (standard set of playing cards) and size 32—a partial deck using cards from each suit but only for ranks 7, 8, 9, 10, Jack, Queen, King, and Ace.

2.0 Findings

Cigital bases its determination on the results of the statistical tests and the inspection of source code. Cigital certifies that the RNG used by REEL complies with best practices for randomness. The random number generator produces unpredictable and statistically random sequences that are used to generate the hands dealt.

Cigital found that the implementation adheres to current best practices in generating random seed values. Source code analysis did not produce any evidence of improper calculations using the random numbers or misuse that would introduce predictability or bias.

In the shuffles of the decks of cards, Cigital found no evidence of bias or predictability. The shuffle test results were statistically significant and correlated strongly with expected probabilities.

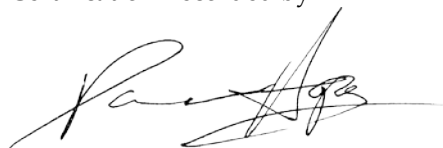
3.0 Validity

This determination of statistical randomness does not extend beyond the software and hardware components examined. These results pertain only to systems composed of the hardware and software that were tested when they are operated in the manner described to Cigital during the evaluation.

4.0 Expiration

This certification expires 31 December, 2014 or when a material change is made to the components of the system that were the subject of this evaluation.

Certification Recorded by:



Paco Hope
Principal Consultant
Cigital Ltd
1 December 2013