BMM Evaluation Report for

Eyecon RNG

Eyecon Alderney Limited

BMM Report Reference: Eyecon.1004.07 - RNG Malta

Date: September 6, 2017

bmm australia pty ltd
suite 107, 35 doody street, p.o. box 6223, alexandria nsw, australia 2015
level 3, 810 whitehorse road, box hill, vic, australia 3128

t +612 8337 6900 f +612 8338 0775
t +613 9895 9888 f +613 9899 6277

corporate reg: ABN 65 084 016 044

bmm.com

TEST REPORT SUMMARY

Client:	Eyecon Alderney Limited Inchalla, Le Val Alderney GY9 3UL
Contact:	Robert Black (robert.black@eyecon.com)
Manufacturer:	Eyecon Alderney Limited
Machine Type:	Random Number Generator
Product Name:	Eyecon RNG
Date of Issue:	6 September 2017
Project Number:	EYECON.1004
BMM Test Report:	EYECON.1004.07 - RNG Malta
Market:	Online
Regulator:	Malta Gaming Authority
Standards Tested to:	Remote Gaming Regulations S.L.438.04
Issues/Observations:	None
BMM Certification:	I, Christopher van Prooije, Systems Consultant, Mathematics, hereby certify that the Random Number Generator used in online gaming complies with the relevant standards and is recommended for approval by the Authority for operation in Malta.

Signed:

Christopher van Prooije, Systems Consultant, Mathematics

1 PURPOSE OF EVALUATION

Eyecon Alderney Limited has requested BMM to evaluate the random number generator (RNG) used in the Eyecon RNG against the Remote Gaming Regulations S.L.438.04.

2 DESCRIPTION OF RNG

The RNG uses an instance of the cryptographically secure Java SecureRandom class. This uses the SHA-1 hash algorithm and a 160-bit state to securely generate random values.

3 BMM EVALUATION PERFORMED

BMM examined the RNG source code and performed statistical tests on the output from the RNG. The source code file(s) used are listed in Appendix A.

3.1 Source Code Review

The RNG is seeded using its own internal seeding mechanisms which draw on multiple hardware and software sources of entropy, ensuring the state is both entirely unpredictable and irreproducible. Methods are provided to produce random numbers in target ranges without introducing any bias. A monitor service runs tests on numbers drawn from the RNG once every minute to detect failures.

3.2 Statistical Testing

Statistical tests were performed on the output from the RNG. Sets of 1 million numbers in the ranges of 32, 52 and 113 were generated 100 times each and tested. 10MB of raw numbers were produced for the Diehard tests, and 1 million numbers were generated for the NIST tests.

The following tests were performed on the data set:

- Frequency – frequency of each number across the entire sample set.
- Pairs Correlation – frequency of each combination of two numbers occurring together.
- Gap – counts of the size of gaps between successive occurrences of numbers across the entire sample set.
- Coupon Collector – counts of how long it takes to collect complete sets of numbers.
- Runs – counts of ascending and descending sequences of numbers.
- Serial Correlation – counts of occurrences of pairs of numbers with specific gaps between them.
- Kolmogorov-Smirnov – test of the linear distribution of the chi-square probability results.
- Diehard tests – a suite of stringent tests on raw output from the RNG.
- NIST tests – a suite of tests from the National Institute of Standards and Technology.

4 TEST RESULTS

Each test produces a p-value, which is the probability of a truly random process producing a test result less than or equal to the current test result. These p-values are expected to be linearly distributed between 0 and 1, with approximately 5% and 1% of the results falling outside of the 95% and 99% confidence intervals respectively. The distribution of p-values was analysed, and the results showed that the RNG's output was indistinguishable from a true random source, passing at the 95% and 99% confidence levels. The following chart shows the distribution of test result probabilities from the statistical tests and confirms their overall linearity.

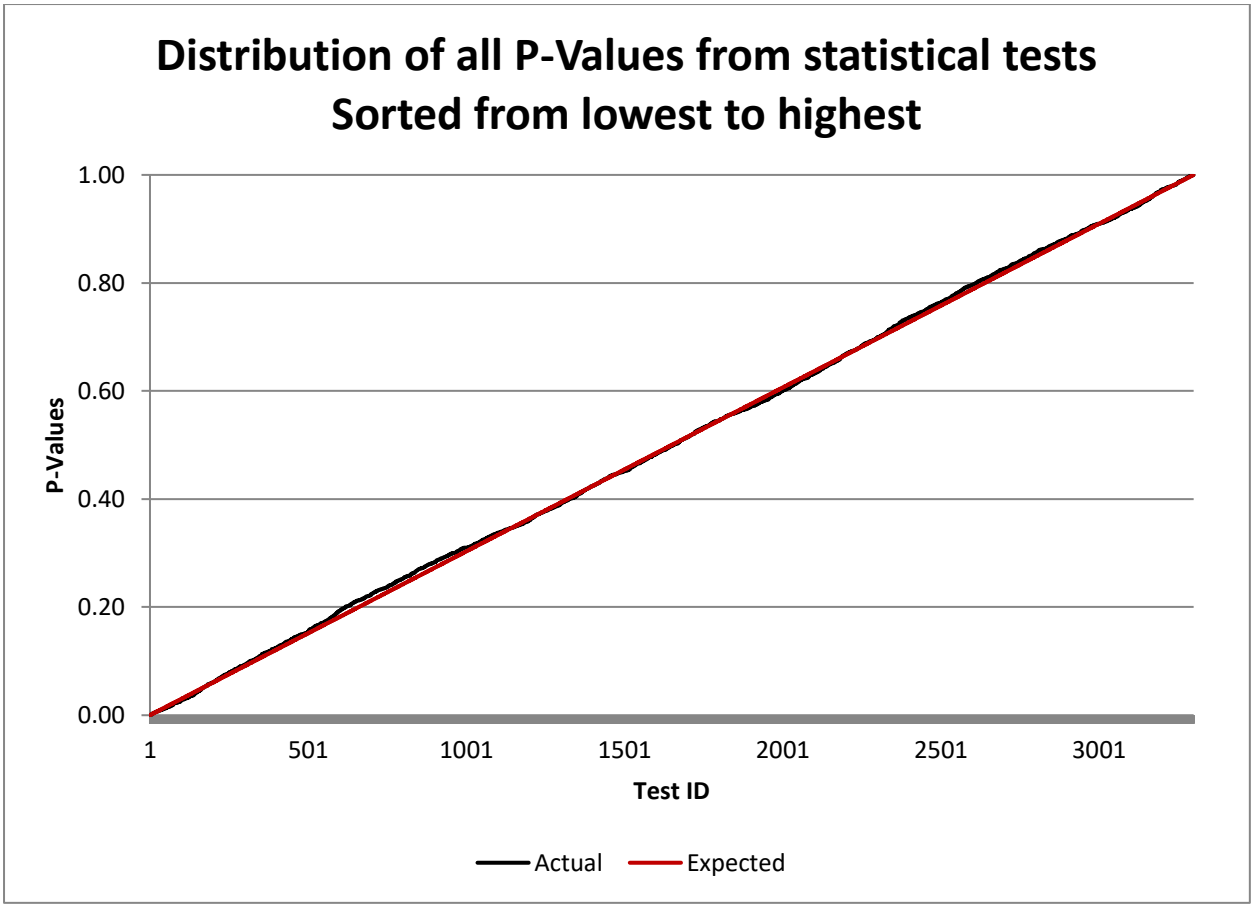

Figure 1: Distribution of result probabilities of tests on output of the RNG

5 CONCLUSION

As a result of statistical testing and source code review, BMM believes that the RNG used by the Eyecon RNG provides uniformly random data suitable for its intended application. This RNG complies with the applicable requirements of the Remote Gaming Regulations S.L.438.04.

APPENDIX A: SOURCE CODE FILES

The following file(s) are used by the RNG. The signature provided is generated using the SHA1 algorithm.

Files	SHA1 Signature
eyecon-rng-1.0.1.jar	D2BFE8EF8FB4F0C33D2988F9A2A030FD66A295F9