| | |
|---|---|
| Evaluation Report: | 3 Oaks Gaming RNG Evaluation for Isle of Man |
| Report Identification: | GNR-IOM-220124-RC-R1 |
| Evaluation Laboratory: | Gaming Associates Europe Ltd<br>www.gamingassociates.com<br>178 Merton High Street<br>London SW19 1AY<br>United Kingdom<br>Office 1, 82 London Road<br>Leicester LE2 0QR<br>United Kingdom<br>123, Melita Street<br>Valletta VLT 1123<br>Malta |
| Supervisor: | Baha Ansari |
| Signatures: | |
| Certifier: | Wajahat Kashan |
| UKAS ISO/IEC 17025 Accreditation No: | 9263 |
| Dates of evaluation work: | 06 January 2022 to 19 January 2022 |
| Date of issue of evaluation report: | 24 January 2022 |
| Report prepared for: | 3 Oaks Gaming<br>Green Rock Ltd<br>Clinch's House, Lord Street, Douglas,<br>Isle of Man, IM99 1RZ, |
| Company Number | 134595C |
| Jurisdiction: | Isle of Man Gambling Supervision Commission |
| Technical Standard used for evaluation: | The Online Gambling Regulation Act 2001, The Online Gambling (System Verification) (No. 2) Regulations 2007 |

# 1 Notations

## 1.1 Confidentiality

This document, all related documents, and methodologies embodied in this document and related documents ("*the documents*") are the property of Gaming Associates Europe Ltd (**ga**). Unauthorised copying and distribution of *the documents*, by any means, on any media is prohibited.

This document, its themes, and ideas are strictly confidential and may not be used in any manner other than its expressed purpose, without the written permission of the author. The document is for client and Isle of Man Gambling Supervision Commission to advise the compliance status of as "the client' or "client" RNG, against The Online Gambling Regulation Act 2001, The Online Gambling (System Verification) (No. 2) Regulations 2007.

*The documents* are copyright.

## 1.2 Disclaimer

**ga** has reported on what it has discovered through evaluation of client's RNG. This report is not an evaluation of the game or interactive gaming system and related processes.

# 2 Administration

## 2.1 Contents

## 2.2 Version

| Version | Description | Date |
|---|---|---|
| V0.1 | Initial draft – MSID | 2022-01-20 |
| V1.0 | QA & release – WKAS | 2022-01-24 |

# 3 Executive summary

## 3.1 Introduction

3 Oaks Gaming has requested Gaming Associates (**ga**) to evaluate their Random Number Generator (RNG) being used in online games against Isle of Man (IoM) Gambling Supervision Commission compliance requirements listed in Schedule 1 of The Online Gambling Regulation Act 2001, The Online Gambling (System Verification) (No. 2) Regulations 2007 [1].

This report presents the results of evaluation performed by **ga** for the RNG against IoM technical standards. Hashes of source code and binary files related to the RNG are listed in ***Annex B :*** of this report.

## 3.2 RNG details

3 Oaks Gaming New object of Random generator creates per GS process with own seed. If process dies, new random object with random seed will be created. The algorithm used for the pRNG is Mersenne Twister generator but have os.urandom as option (On a Unix-like system, random bytes are read from the /dev/urandom device) .

## 3.3 Scope of evaluation

The scope of evaluation of RNG is Schedule 1 requirements of The Online Gambling Regulation Act 2001, The Online Gambling (System Verification) (No. 2) Regulations 2007. The evaluation included review of implementation of RNG, source code review, and statistical analysis of the output of RNG.

## 3.4 Conclusions and Recommendations

The current implementation of 3 Oaks Gaming RNG complies with Schedule 1 requirements of The Online Gambling Regulation Act 2001, The Online Gambling (System Verification) (No. 2) Regulations 2007.

**ga** concludes and recommends that the current implementation of the 3 Oaks Gaming RNG is suitable for use in online games and meets IoM RNG requirements.

# 4 Test Results

This section summarises the results of the tests performed on 3 Oaks Gaming RNG. The tables in the following sub-sections provide the compliance status of the RNG against IoM RNG requirements listed in [1]. Different values used in the compliance status column are described as follows:

**Comply**: The RNG complies with the requirement.

**Pending:** The requirement could not be verified at the time of RNG evaluation.

**Acknowledged:** The requirement is only a statement or information.

**N/A**: The requirement is not applicable to the RNG.

**Out of scope**: The requirement cannot be evaluated at this stage due to the current scope of testing or limitation of test environment.

## 4.1 Schedule 1 - System verification requirements

| IoM Requirements | System Compliance | Comments/Anomalies |
|---|---|---|
| **SCHEDULE 1 - REQUIREMENTS WITH WHICH SYSTEMS MUST COMPLY FOR<br>GAMING AND LOTTERIES** | | |
| (3) The System must satisfy the following criteria for randomness for any Gaming or Lottery (save where different rules apply and have been approved by the Commissioners and published to the Participant or potential Participant prior to its participation), following Schneier:- | | |
| (a) the data must be randomly generated, passing appropriate statistical non static output results tests of randomness (e.g., Marsaglia's "Diehard" set of tests) uniformly distributed over the set range; | Comply | 3 Oaks Gaming The algorithm is used for the pRNG is Mersenne Twister generator but have os.urandom as option (On a Unix-like system, random bytes are read from the /dev/urandom device) .<br>The raw and scaled random data generated by the RNG is found to be random and uniformly distributed.<br>See "Annex A: Statistical testing of RNG output" for details. |
| (b) the data must be unpredictable, i.e. it must not be computationally feasible to predict what the next number will be, given complete knowledge of the algorithm or hardware generating the sequence, and all previously generated numbers; and | Comply | Random generator creates per GS process with own seed. If process dies, new random object with random seed will be created the random numbers generated by the pRNG cannot be reproduced as seed. |
| (c) the series cannot reliably be reproduced, i.e. if the sequence generator is activated again with the same input (as exactly as humanly possible) it will produce two completely unrelated random sequences. | Comply | The same series of random numbers cannot be reproduced due to random seeding and use of GS process. |
| (4) The Operator must disclose the methodology of any random seeding and any seeding must be proven to result in an unpredictable output. | Comply | Random generator creates per GS process with own seed. If process dies, new random object with random seed will be created the random numbers generated by the pRNG cannot be reproduced as seed |
| (5) The outcome of any Game or Lottery, as the case may be, and the return to the Participant, must be | Comply | The game outcomes are only based on the random numbers generated by RNG in conjunction with the |

| IoM Requirements | System Compliance | Comments/Anomalies |
|---|---|---|
| independent of the CPU, memory, disk or other components used in the computer or other device used by the Participant. | | game rules. Verification of game rules is out of scope of this evaluation. |
| (6) The Game or Lottery outcome, as the case may be, must not be affected by the effective bandwidth, link utilisation, bit error rate or other characteristic of the communications channel between the System and the computer or other device used by the Participant. | Comply | The game outcomes are only based on the random numbers generated by RNG in conjunction with the game rules. Verification of game rules is out of scope of this evaluation. |

# 5 References

1. The Online Gambling Regulation Act 2001, The Online Gambling (System Verification) (No. 2) Regulations 2007.

## Annex A : Statistical testing of RNG output

Statistical analysis of RNG output has been performed for:

- Raw (binary) pRNG output; and
- Scaled pRNG output for games served by the RNG.

This annexure provides results of the statistical analysis.

### A.1 Diehard test results (raw RNG output)

Following table presents the summary of diehard test results. These tests were applied on raw output of pRNG generated by the test harness by 3 Oaks Gaming. The data has passed all the tests in the diehard battery of tests. The pRNG is considered to have overall passed the diehard tests with 99% confidence interval

**Data file: Rawdata1.data**

| Test No. | Description | p-value | Test results (Pass/Fail) |
|---|---|---|---|
| 1 | BIRTHDAY SPACINGS TEST | 0. 571415 | Pass |
| 2 | BINARY RANK TEST for 31x31 matrices | 0. 902496 | Pass |
| 3 | BINARY RANK TEST for 32x32 matrices | 0. 385224 | Pass |
| 4 | BINARY RANK TEST for 6x8 matrices | 0. 977358 | Pass |
| 5 | BITSTREAM TEST | 0. 556982 | Pass |
| 6 | Overlapping Pairs-Sparse-Occupancy (OPSO) Test | 0. 547265 | Pass |
| 7 | Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test | 0. 47815 | Pass |
| 8 | DNA test | 0.490770 | Pass |
| 9 | COUNT-THE-1's TEST | | |
| | (i) byte stream for 2549.59 chi-square value | 0. 758448 | Pass |
| | (ii) byte stream for 2492.78 chi-square value | 0. 459321 | Pass |
| 10 | COUNT-THE-1's TEST for specific bytes | 0.586613 | Pass |
| 11 | PARKING LOT TEST | 0. 783975 | Pass |
| 12 | MINIMUM DISTANCE TEST | 0. 338061 | Pass |
| 13 | 3DSPHERES TEST | 0. 347259 | Pass |
| 14 | SQEEZE TEST | 0. 231966 | Pass |
| 15 | OVERLAPPING SUMS test | 0. 506370 | Pass |
| 16 | THE RUN TEST | | |
| | (i) Runs up Test | 0. 042790 | Pass |
| | (ii) Runs Down Test | 0. 683496 | Pass |
| | (iii) Runs up Test | 0. 682297 | Pass |
| | (iv) Runs Down Test | 0. 140863 | Pass |
| 17 | CRAPS TEST | | |

| Test No. | Description | p-value | Test results (Pass/Fail) |
|---|---|---|---|
| | (i) No. of wins | 0. 768566 | Pass |
| | (ii) for throws/game | 0. 298778 | Pass |
| 18 | OVERLAPPING 5-PERMUTATION TEST | | |
| | (i) Sample of 1,000,000 consecutive 5-tuples | 0. 635268 | Pass |
| | (ii) Sample of 1,000,000 consecutive 5-tuples | 0. 078592 | Pass |

## Data file: Rawdata2.data

| Test No. | Description | p-value | Test results (Pass/Fail) |
|---|---|---|---|
| 1 | BIRTHDAY SPACINGS TEST | 0. 748224 | Pass |
| 2 | BINARY RANK TEST for 32x32 matrices | 0. 500398 | Pass |
| 3 | BINARY RANK TEST for 31x31 matrices | 0. 606425 | Pass |
| 4 | BINARY RANK TEST for 6x8 matrices | 0. 079764 | Pass |
| 5 | BITSTREAM TEST | 0.461091 | Pass |
| 6 | Overlapping Pairs-Sparse-Occupancy (OPSO) Test | 0.388604 | Pass |
| 7 | Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test | 0.679464 | Pass |
| 8 | DNA test | 0.445383 | Pass |
| 9 | COUNT-THE-1's TEST | | |
| | (i) byte stream for 2475.62 chi-square value | 0. 365131 | Pass |
| | (ii) byte stream for 2523.61 chi-square value | 0. 630798 | Pass |
| 10 | COUNT-THE-1's TEST for specific bytes | 0.536258 | Pass |
| 11 | PARKING LOT TEST | 0. 537076 | Pass |
| 12 | MINIMUM DISTANCE TEST | 0. 149420 | Pass |
| 13 | 3DSPHERES TEST | 0. 721184 | Pass |
| 14 | SQEEZE TEST | 0. 200846 | Pass |
| 15 | OVERLAPPING SUMS test | 0. 445290 | Pass |
| 16 | THE RUN TEST | | |
| | (i) Runs up Test | 0. 046670 | Pass |
| | (ii) Runs Down Test | 0. 852398 | Pass |
| | (iii) Runs up Test | 0. 146116 | Pass |
| | (iv) Runs Down Test | 0. 818765 | Pass |
| 17 | CRAPS TEST | | |
| | (i) No. of wins | 0. 541216 | Pass |

| Test No. | Description | p-value | Test results (Pass/Fail) |
|---|---|---|---|
| | (ii) for throws/game | 0. 953812 | Pass |
| 18 | OVERLAPPING 5-PERMUTATION TEST | | |
| | (i) Sample of 1,000,000 consecutive 5-tuples | 0. 762189 | Pass |
| | (ii) Sample of 1,000,000 consecutive 5-tuples | 0. 948793 | Pass |

## A.2 Scaled data statistical testing results

The following tables describe the results of statistical testing performed on scaled data used to generate game results. The scaled data was generated using the RNG being evaluated.

The data passed all statistical tests within 99% confidence interval which confirms that the game outcomes are random and uniformly distributed over the range required by the games.

### Data file name: Data1.txt (Scaling range: 0 to 36)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 1,000,000 | 3.8070e+001 | Pass |
| Runs-up | 1,000,000 | 1.9123e-003 | Pass |
| Runs-down | 1,000,000 | 2.0041e-003 | Pass |

### Data file name: Data2.txt (Scaling range: 0 to 36)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 1,000,000 | 4.3673e+001 | Pass |
| Runs-up | 1,000,000 | 1.8659e-003 | Pass |
| Runs-down | 1,000,000 | 1.9995e-003 | Pass |
| Correlation Test | 1,000,000 | 1.8590e-003 | Pass |

### Data file name: Data1.txt (Scaling range: 0 to 51)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 3,000,000 | 5.3231e+001 | Pass |
| Runs-up | 3,000,000 | 1.2540e-003 | Pass |
| Runs-down | 3,000,000 | 1.1982e-003 | Pass |

### Data file name: Data2.txt (Scaling range: 0 to 51)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 3,000,000 | 5.6248e+001 | Pass |
| Runs-up | 3,000,000 | 1.2108e-003 | Pass |
| Runs-down | 3,000,000 | 1.1611e-003 | Pass |
| Correlation Test | 3,000,000 | 9.9012e-004 | Pass |

### Data file name: Data1.txt (Scaling range: 0 to 99)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 3,000,000 | 9.4022e+001 | Pass |
| Runs-up | 3,000,000 | 4.2356e-004 | Pass |
| Runs-down | 3,000,000 | 4.1960e-004 | Pass |

### Data file name: Data2.txt (Scaling range: 0 to 99)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 3,000,000 | 1.1716e+002 | Pass |
| Runs-up | 3,000,000 | 4.0259e-004 | Pass |
| Runs-down | 3,000,000 | 4.3300e-004 | Pass |
| Correlation Test | 3,000,000 | -1.4725e-003 | Pass |

## Data file name: Data1.txt (Scaling range: 0 to 774)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 1,000,000 | 8.0787e+002 | Pass |
| Runs-up | 1,000,000 | 1.3441e-004 | Pass |
| Runs-down | 1,000,000 | 1.4644e-004 | Pass |

## Data file name: Data2.txt (Scaling range: 0 to 774)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 1,000,000 | 7.5981e+002 | Pass |
| Runs-up | 1,000,000 | 1.5268e-004 | Pass |
| Runs-down | 1,000,000 | 1.6690e-004 | Pass |
| Correlation Test | 1,000,000 | -4.5243e-004 | Pass |

## Data file name: Data1.txt (Scaling range: 0 to 499999)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 1,000,000 | 4.9953e+005 | Pass |
| Runs-up | 1,000,000 | 1.5152e-004 | Pass |
| Runs-down | 1,000,000 | 1.5910e-004 | Pass |

## Data file name: Data2.txt (Scaling range: 0 to 499999)

| Statistical test | Sampling size | Sum of square of residuals | Pass/Fail |
|---|---|---|---|
| Chi-Square | 1,000,000 | 4.9762e+005 | Pass |
| Runs-up | 1,000,000 | 1.6402e-004 | Pass |
| Runs-down | 1,000,000 | 1.3486e-004 | Pass |
| Correlation Test | 1,000,000 | 8.2701e-004 | Pass |

# Annex B : Hashes of RNG source code and binary

SHA-1 hashes of files related to the 3 Oaks Gaming RNG have been taken to establish a baseline of the system evaluated by **ga**. The hashes are listed below.

| | |
|---|---|
| rng.py | c833b0d5cafccf72281fab1398e0be58a6fe69c8 |
| mersenne_twister.py | 03a7f81f656a6d8754132bb7e682acc843d79218 |

# End of document