

Evaluation Report: 3 Oaks Gaming RNG Evaluation Report for Sweden

Report Identification: GNR-SE-220525-01-RC-R1

Testing Laboratory:



178 Merton High Street
London SW19 1AY
United Kingdom
Office 1, 82 London Road
Leicester LE2 0QR
United Kingdom
123, Melita Street
Valletta VLT 1123
Malta

Supervisor: Baha Ansari

Signatures:

Evaluator: Wajahat Kashan

UKAS ISO/IEC 17025
Accreditation No. 9263

Dates of testing work: 09 May 2022 to 18 May 2022

Date of issue of test report: 25 May 2022

Report prepared for: 3 Oaks Gaming (Green Rock Ltd)

Address: Clinch's House, Lord Street,
Douglas, IM99 1RZ,
Isle of Man

Jurisdiction: Spelinspektionen (Swedish Gaming Authority)
Kingdom of Sweden

Technical Standard used for testing: SFS 2018:1138 Gambling Act, 14 June 2018.
SFS 2018:1475 Gambling Ordinance, 5 July 2018.
LIFS 2018:8 Regulations and Guidelines on Technical Requirements and Accreditation of Organisations for Inspection, Testing and Certification of Gambling Service Providers, 25 July 2018.

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 (hereinafter referred to as Gaming Associates or **ga**). Unauthorized 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 documents are for the intended client named in this report, also referred to as "the client" or "client", and the applicable gaming jurisdiction mentioned in this document.

The documents are copyright.

1.2 Disclaimer

ga has reported on what it has discovered throughout the assessment period of the client's RNG related to the technical scope of testing as per applicable jurisdictional requirements. Results are based on the client's submission of information material, source code, and access to the testing environment, and applicable testing is performed within a finite period.

Inherently there are limitations in performing compliance testing within a laboratory environment and accordingly, **ga** has undertaken its best endeavours to ensure a thorough assessment is performed and a conclusion stated.

2 Administration

2.1 Contents

1	Notations	2
1.1	Confidentiality	2
1.2	Disclaimer.....	2
2	Administration	3
2.1	Contents.....	3
2.2	Version.....	3
3	Executive summary	4
3.1	Introduction	4
3.2	RNG system details	4
3.3	Scope of evaluation	4
3.4	Conclusions and Recommendations	4
4	Test Results	5
4.1	LIFS2018:8 Chapter 13 - Functional requirements for RNGs.....	5
5	References.....	8
Annex A : Statistical testing of output of RNG		9
A.1	Diehard test results (raw RNG output)	9
A.2	Scaled data statistical testing results.....	11
Annex B : Hashes of RNG source code and binary		14
End of document.....		15

2.2 Version

Version	Description	Date
V0.1	Initial draft – MSID	2022-05-19
V0.2	Reviewed & Updated – WKAS	2022-05-20
V0.3	QA – BANS	2022-05-23
V1.0	Final report to 3 Oaks Gaming	2022-05-25

3 Executive summary

3.1 Introduction

3 Oaks Gaming has requested Gaming Associates (**ga**) to evaluate their Random Number Generator (RNG) against the applicable requirements of the Swedish Gaming Authority (SGA) as regulated by Spelinspektionen. **ga** is accredited by UKAS (accreditation no. 9263) as a testing laboratory in accordance with the international standard ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories.

This report presents the results of testing performed by **ga** related to the technical scope of testing as per applicable jurisdictional requirements. Hashes of binary files SHA-1 of the critical part of the software that use the Java RNG are given Annex B.

3.2 RNG system 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 was tested against the following game-related requirements of the SGA's technical standards:

- ♠ SFS 2018:1138 Gambling Act, 14 June 2018,
- ♠ SFS 2018:1475 Gambling Ordinance, 5 July 2018,
- ♠ LIFS 2018:8 Regulations and Guidelines on Technical Requirements and Accreditation of Organisations for Inspection, Testing, and Certification of Gambling Service Providers, 25 July 2018,

Evaluation of the RNG was performed against "Chapter 13 – Functional requirements for random number generators" of LIFS 2018:8 technical requirements in accordance with ISO/IEC 17025:2005 standard.

3.4 Conclusions and Recommendations

Subject to the scope of testing and on the basis of testing performed of 3 Oaks Gaming RNG **ga** has formed an opinion that the submitted RNG complies with the applicable technical standards of the jurisdiction of Sweden as regulated by the Swedish Gaming Authority (Spelinspektionen).

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 assessment of compliance status of the RNG against the applicable requirements of the technical standards of the jurisdiction of Sweden as regulated by the SGA (Spelinspektionen).

The different values used in the tables below within 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 LIFS2018:8 Chapter 13 - Functional requirements for RNGs

SGA Req #	Spelinspektionen (SGA) Requirements	Compliance Status	Comments/Anomalies
Chapter 13	Functionality Requirements for Random Number Generators		
§ 1	The results from a random number generator must be random, statistically independent, have a correct standard deviation and correct probability distribution.	Compliant	3 Oaks Gaming uses 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) algorithm to produce random numbers for games. The data output of pRNG passed statistical tests demonstrating that the data is statistically independent
	The results yielded by the random number generator must not be predictable without knowledge of the applied algorithm, implementation and initial values. General advice: <i>There are several statistical tests that can be used to ascertain the results of a random number generator. The DIEHARD test suite (Marsaglia) and the NIST test suite (National Institute of Standards and Technology) are two of the tests that can be used.</i>	Compliant	The random numbers generated by 3 Oaks Gaming RNG are not predictable. The data output of RNG passed statistical tests. The results are mentioned in Annex A.
§ 2	There must be a documented reference to a well-established algorithm and any source code as well as to the recalculation procedure of the random number generator.	Compliant	3 Oaks Gaming is used Mersenne Twister generator but have os.urandom as option (On a Unix-like system, random bytes are read from the /dev/urandom device) algorithm is used in the pRNG and documentation is defined which explains the technical aspects of the RNG.
	If the random number generator is built in to the software, it must be possible to present the entire source code, along with comments and documentation.	Compliant	PRNG of 3 Oaks Gaming is software that is built into the gaming server to generate the random numbers for the games.

SGA Req #	Spelinspektionen (SGA) Requirements	Compliance Status	Comments/Anomalies
	General advice: <i>The algorithm that the random number generator is based on should be published in an internationally recognised publication.</i> <i>The outcome tests that may be used on generated random numbers include the X2 test (chi-squared-test), the autocorrelation test and the runs test.</i> <i>The licence holder can enable verification of the set payout table by having the accredited body or the Swedish Gambling Authority to review programmes, plates, logs, verification lists or other documentation for the payout table.</i>		
§ 3	The random number generator must be able to withstand the set maximum load.	Compliant	RNG can easily handle heavy loads and works efficiently.
§ 4	Functions that do not generate outcomes in games but which depend on random elements must be based on the results of the random number generator. General advice: <i>Such functions may include a randomized sequence or placement at a poker table during a tournament.</i>	Compliant	The random number generator results are used to produce game results.
§ 5	Calculations based on a random number generator must have a correct standard deviation and correct probability distribution.	Compliant	The scaled random numbers passed statistical tests and comply with this requirement.
	The numbers, symbols or events resulting from the random number generator must correspond with the rules set for the game involved. General advice: <i>If the random numbers are translated into cards, for examples, there should be four aces, four kings, etc. in a normal deck, if the game uses a normal deck.</i>	Out of scope	Random numbers mapping with the game symbols is part of games testing.
§ 6	The calculations of the random number generator must correspond to the events registered in the gambling system.	Compliant	Numbers generated by the RNG are mapped to the game symbols and all the game outcomes are recorded in the gaming system.
§ 7	If the rules of the game requires a sequence from a random number generator to be set in advance, it is only allowed to generate new sequences if this is stated in the rules.	Out of scope	Out of scope of RNG evaluation.
§ 8	Unless otherwise specified in the rules of the game, the results from a random number generate must always be independent of events in the current or previous games.	Out of scope	Out of scope of RNG evaluation.
	Drawing Equipment Without Random Number Generators		
§ 9	The results from drawing equipment without a random number generator must be random, statistically independent, have a correct standard deviation and correct probability distribution. General advice: <i>The outcome tests that may be used on generated random numbers include the X2 test</i>	N/A	3 Oaks Gaming utilizes RNG for producing game results. No drawing equipment is used.

SGA Req #	Spelinspektionen (SGA) Requirements	Compliance Status	Comments/Anomalies
	<i>(chi- squared-test), the autocorrelation test and the runs test.</i>		
§ 10	Independent drawing equipment without a random number generator must be kept locked in with limited access.	N/A	3 Oaks Gaming utilizes RNG for producing game results. No drawing equipment is used.
	Drawing Equipment for Live Casino Games		
§ 11	Drawing equipment used in live casino games must be monitored and recorded.	N/A	3 Oaks Gaming does not offer live casino games.
	The recorded material must show compliance with the rules of the game.		
	The recording must register date and time.		
§ 12	There must be physical access control for the premises used for live casino games and any associated areas.	N/A	3 Oaks Gaming does not offer live casino games.
	There must separate access control, at least for different employee categories. General advice: <i>Dealer, floor manager, supervisor, surveillance staff are examples of various types of employees that should be categorised into different authorisation groups.</i>		

5 References

1. SFS 2018:1138 Gambling Act, 14 June 2018.
2. SFS 2018:1475 Gambling Ordinance, 5 July 2018.
3. LIFS 2018:8 Regulations and Guidelines on Technical Requirements and Accreditation of Organisations for Inspection, Testing and Certification of Gambling Service Providers, 25 July 2018.

Annex A : Statistical testing of output of RNG

Statistical analysis of RNG output has been performed for:

- ♠ Raw (binary) RNG output; and
- ♠ Scaled RNG 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 RNG generated by the test harness provided by 3 Oaks Gaming (3 Oaks Gaming). The data has passed the tests in the diehard battery of tests with 99% confidence interval.

Data file: raw_1.txt

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 2462.49 chi-square value	0. 758448	Pass
	(ii) byte stream for 2568.76 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	SQUEEZE 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

Test No.	Description	p-value	Test results (Pass/Fail)
17	CRAPS TEST		
	(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: raw_2.txt

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0. 748224	Pass
2	BINARY RANK TEST for 31x31 matrices	0. 500398	Pass
3	BINARY RANK TEST for 32x32 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 2381.93 chi-square value	0. 365131	Pass
	(ii) byte stream for 2528.87 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	SQUEEZE 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
	(ii) for throws/game	0. 953812	Pass

Test No.	Description	p-value	Test results (Pass/Fail)
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

Degree of Freedom: 36

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
36	Data1.txt	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

Degree of Freedom: 36

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
36	Data2.txt	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 between "Data1.txt" and "Data2.txt"

Sampling size	correlation coefficient	Pass/Fail
1,000,000	1.8590e-003	Pass

Data File Name: Data1.txt

Degree of Freedom: 51

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
51	Data1.txt	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

Degree of Freedom: 51

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
51	Data2.txt	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 between "Data1.txt" and "Data2.txt"

Sampling size	correlation coefficient	Pass/Fail
3,000,000	9.9012e-004	Pass

Data File Name: Data1.txt
Degree of Freedom: 99

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
99	Data1.txt	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
Degree of Freedom: 99

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
99	Data2.txt	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 between “Data1.txt” and “Data2.txt”

Sampling size	correlation coefficient	Pass/Fail
3,000,000	-1.4725e-003	Pass

Data File Name: Data1.txt
Degree of Freedom: 774

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
774	Data1.txt	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
Degree of Freedom: 774

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
774	Data2.txt	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 between “Data1.txt” and “Data2.txt”

Sampling size	correlation coefficient	Pass/Fail
1,000,000	-4.5243e-004	Pass

Data File Name: Data1.txt
Degree of Freedom: 499999

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
499999	Data1.txt	Chi-Square	10,000,000	4.9953e+005	Pass
		Runs-up	10,000,000	1.5152e-004	Pass
		Runs-down	10,000,000	1.5910e-004	Pass

Data File Name: Data2.txt
Degree of Freedom: 499999

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
499999	Data2.txt	Chi-Square	10,000,000	4.9762e+005	Pass
		Runs-up	10,000,000	1.6402e-004	Pass
		Runs-down	10,000,000	1.3486e-004	Pass

Correlation between “Data1.txt” and “Data2.txt”

Sampling size	correlation coefficient	Pass/Fail
10,000,000	8.2701e-004	Pass

Annex B : Hashes of RNG source code and binary

SHA1-hashes av pRNG är listade i tabellen nedan:

File name	Description	SHA1
rng.py	common library methods for RNG	c833b0d5cafccf72281fab1398e0be58a6fe69c8
mersenne_twister.py	common library of RNG source files	03a7f81f656a6d8754132bb7e682acc843d79218

End of document