



Certification Report: ITL2301920

Orbital Gaming

Random Number Generator Certification Report Malta Gaming Authority


29 June 2023

This test report may not be reproduced, other than in full, except with the prior written permission from iTech Labs.

This test report is valid only for the intended jurisdiction as stated in this report and has no legal value in any other jurisdiction.

Certification Report: ITL2301920

1 Test Laboratory details

Nº	Description	Details
1.	Contact Details of Test Laboratory	iTech Labs Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia URL: www.itechlabs.com E-mail: info@itechlabs.com
2.	Physical location of where testing was performed	iTech Labs, Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia
3.	Date Commenced	17 May 2023
4.	Date Completed	29 June 2023
5.	Scope of Work	Certification of the new software RNG for the software provider, Orbital Gaming
6.	Result	Passed all tests, subject to Section 5 Final declaration and conformity, Item 1 Conditions.
7.	Other	None
8.	Test Supervisor Signature:	 Kiren Sreekumar, Principal Consultant, iTech Labs

2 Executive summary

2.1 General Information

Nº	Description	Details
1.	Identification	Orbital Gaming RNG
2.	Type of system	Online Casino
3.	Games using this RNG	Non-card games: Instant Games, Keno and Slots Card games: Single Deck (without joker) and Two Decks (without joker)
4.	Target Jurisdiction	Malta
5.	Guidelines used for testing	Malta Remote Gaming Regulations S.L.438.04.
6.	Software provider	Name: Orbital Gaming Address: Tbilisi, Georgia URL: https://orbitalgaming.com/ Contact: Irakli Menabde Email: irakli@orbitalgaming.com
7.	Operator details	Operator Name: N/A Address: N/A URL: N/A Contact: N/A Email: N/A

2.2 Description of RNG

2.2.1 Software Details

Nº	Description	Details
1.	RNG type	Pseudo Random Number Generator (PRNG)
2.	Implementation language	Go



Certification Report: ITL2301920

N°	Description	Details
3.	RNG version number	2.0
4.	RNG build number	2.0
5.	Superseded RNG	The RNG has not been previously certified.
6.	RNG algorithm	HMAC SHA512
7.	Period of algorithm	Indeterminate since it is hash based
8.	Dimension of numbers from algorithm	512 bits
9.	Seeding	Seeding is done from combination of the entropy listed below: /dev/urandom in linux environment. /dev/urandom, by its design, gathers environmental noise from device drivers and other sources into an entropy pool.
10.	Reseeding	No Reseeding
11.	Library name and version	The RNG uses Golang library-based implementation. Hence the RNG certification is restricted to Golang version 1.18.9.
12.	Operating system	Linux
13.	Environmental particulars	Platform supplier hosting the RNG: Cloud9 (Private Cloud Company) Platform version hosting the RNG: OS: CentOS 7, Kernel: 3.10.0-1160.36.2.el7.x86_64 (Kernel version may be upgraded as part of CentOS updates channel), go version go1.18.9 linux/amd64
14.	Files and SHA-1 hashes	Refer to Section 2.3 Critical Components of RNG Table 1 and Table 2 below for the list of hashes of source code files and binaries (if applicable) of the RNG.

2.2.2 Hardware Details

Not Applicable, software RNG.

2.3 Critical Components of RNG

Table 1: SHA-1 Signature of RNG source files

File Name	Size (bytes)	SHA-1
pf.go	2,100	e83c1ff2aee19b642c5885f9468d856d691c3c77
random.go	1,576	f89ecbd692015ae6cb1fe944d795053690616cda

Table 2: SHA-1 Signature of executables

File Name	Size (bytes)	SHA-1
rng	15,660,167	5582bc34cebbdad50dc3dbbe0a6e4cec0de3daff

2.4 Scope of Testing

N°	Description	Details
1.	Vendor supplied output testing	Not Applicable
2.	Test Laboratory generated output from vendor supplied source	Source files were compiled by iTech Labs using the source code supplied by the customer. Refer to Section 2.3 Critical Components of RNG.
3.	Source code review	The source code review verified that the implementation of the RNG is in accordance with the technical requirements. This includes, but is not limited to: a) Identification of algorithm; b) Security of internal state, seeding and re-seeding, thread safety; c) Scaling for Instant Games, Keno and Slots games;

Certification Report: ITL2301920

Nº	Description	Details
		d) Shuffling for Single Deck (without joker) and Two Decks (without joker) games.
4.	Statistical tests	The statistical tests undertaken by iTech Labs are: a) Diehard tests b) Chi-square tests
5.	Theoretical basis of algorithm and supporting crypto-analysis evidence	Literature is readily available, describing the theoretical basis of the algorithm (refer to Section 2.2) Wikipedia article on SHA-2 series of Hash algorithms (SHA-512 is a part of this): https://en.wikipedia.org/wiki/SHA-2 NIST paper "Recommendation for Random Number Generation Using Deterministic Random Bit Generators" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf (SHA-512 is recommended hashing algorithms in section 10.1 of NIST.SP.800-90Ar1.pdf)

2.5 Limitation of use of RNG

Nº	Description	Details
1.	Acceptable degrees of freedom (DOF) permitted	Acceptable DOF's are listed in Section 3.1 Item 5 (below).
2.	Dependency on operating system functionality	None
3.	Library-based implementation	The RNG uses Golang library-based implementation. Hence the RNG certification is restricted to Golang version 1.18.9.
4.	Other	None

3 Detailed test results

3.1 Tests methodology

The testing methodologies listed below were used to ensure the RNG complies with the relevant jurisdictional technical requirements and the scope of work.

Nº	Test Performed	Test Methodology	Result
1.	Review of RNG documentation	Review of RNG documentation was conducted to understand the implementation of RNG in the gaming system.	Comply
2.	Research conducted about RNG algorithm/ hardware	Research conducted about the RNG algorithm to ensure there is no publicly known weakness or vulnerabilities associated with the RNG under evaluation.	Comply
3.	Review of source code	Review of source code was conducted to verify that the implementation of the RNG is in accordance with the technical requirements.	Comply
4.	Statistical testing of raw output of RNG.	Marsaglia's diehard tests were applied to 80 million bits of raw 32 bit random numbers generated by the algorithm. The following diehard tests were conducted on 2 sets of 80 million bits; i. BIRTHDAY SPACINGS ii. OVERLAPPING 5-PERMUTATIONS iii. BINARY RANK TEST for 31x31 matrices iv. BINARY RANK TEST for 32x32 matrices v. BINARY RANK TEST for 6x8 matrices vi. BITSTREAM TESTS ON 20-BIT Words vii. BITSTREAM TESTS OPSO, OQSO, DNA viii. COUNT-THE-1's IN A STREAM OF BYTES ix. COUNT-THE-1's IN SPECIFIC BYTES x. PARKING LOT TEST	Comply Refer Section 4.1 for results.

Certification Report: ITL2301920

N°	Test Performed	Test Methodology	Result
		xi. MINIMUM DISTANCE TEST xii. THE 3DSPHERES TEST xiii. THE SQUEEZE TEST xiv. OVERLAPPING SUMS TEST xv. RUNS TEST xvi. CRAPS TEST	
5.	Statistical testing of scaled / shuffled data	Chi-square tests were conducted for the following: DOF for Single deck (without joker) Cards/Deal: 52 Suits: 156 Ranks: 624 Cards: 2652 DOF for Two decks (without joker) Cards/Deal: 104 Suits: 312 Ranks: 1248 Cards: 5304 DOF for Instant Games (Range: 2):1 DOF for Instant Games (Range: 8): 7 DOF for Instant Games (Range: 9): 8 DOF for Instant Games (Range: 16): 15 DOF for Instant Games (Range: 25): 24 DOF for Instant Games (Range: 96): 95 DOF for Keno (Range: 1 to 40, drawn 10): 390 DOF for Keno (Range: 1 to 80, drawn 10): 790 DOF for Slot (Range: 100000): 99999	Comply Refer Section 4.2 for results
6.	Other	The above test results apply to the code provided by the customer as specified in section 2.3.	-

Note: Evaluation was conducted at iTech Labs facilities in Australia, India and Bulgaria. All functional tests (if any) were conducted remotely (i.e. remote test environment hosted on customer's site).

3.2 Compliance to technical standards

N°	Requirement Description	Results	Comments
3rd Schedule Regulation 25			
3.	The gaming machine must satisfy the randomness following Schneier:		
	(a) the data must be randomly generated, passing appropriate statistical tests of randomness;	Comply	
	(b) the data must be unpredictable, i.e. it must be computationally infeasible to predict what the next number will be, given complete knowledge of the algorithm or hardware generating the sequence, and all previously generated numbers;	Comply	
	(c) the series cannot be reliably reproduced, i.e. if the sequence generator is activated again with the same input (as exactly as is reasonably possible) it will produce two completely unrelated random sequences.	Comply	



Certification Report: ITL2301920

4 Statistical test results

4.1 Testing results for raw output of RNG

The Diehard tests were performed on two random sequences. The columns 'Result Random sequence-1' and 'Result Random sequence-2' contain the filenames for the detailed results. These files are supplied as attachments with this Certification report.

Confidence Level for the tests is: 95%

Overall result: Pass

Result Random sequence-1	Result Random sequence-2	Sample size	Confidence level	Result
Refer to attachment Orbital1.txt	Refer to attachment Orbital2.txt	80 million bits	95%	Pass

4.2 Testing results for scaled/ shuffled data

The Chi-square tests were performed with the results listed in Appendix A. The columns 'Result Datafile1' and 'Result Datafile 2' contain the filenames for the detailed results. These files are supplied with this Certification report.

Confidence Level for the tests is:95%

Overall result: Pass

5 Final declaration and conformity

Nº	Description	Details
1.	Conditions/Observations	The RNG certification is restricted to Golang version 1.18.9.
2.	Certification	<p>Certification Date: 29 June 2023 Software Provider: Orbital Gaming Software Provider site URL: https://orbitalgaming.com Operator Name: N/A Operator site URL: N/A</p> <p>This is to certify that iTech Labs has evaluated the Random Number Generator (RNG) by Orbital Gaming and found that the RNG complies with the relevant standards and is in conformity to the Malta Remote Gaming Regulations S.L.438.04.</p> <p>It is hereby certified that the Random Number Generator (RNG) as specified in Section 2.3, and used by the games listed in Section 2.1 Item 3, is compliant with the technical requirements set in the Third Schedule of the Malta Remote Gaming Regulations S.L.438.04 and that the Random Number Generator (RNG) was tested as an integral part of the gaming system.</p>



Certification Report: ITL2301920

6 Conclusion

While it is not possible to test all possible scenarios in a laboratory environment, iTech Labs has conducted a level of testing appropriate for a submission of this type.

Accordingly, subject to the above comment, iTech Labs certifies that the items under test comply with the relevant Technical Standards, unless otherwise stated.

Signatures:

Geoff Nicoll
Principal Consultant
iTech Labs
29 June 2023

Kiren Sreekumar
Principal Consultant
iTech Labs
29 June 2023



Certification Report: ITL2301920

Appendix A – Chi Square Testing Result (refer to Section 4.2)

Table A.1 Non Card Games

Game Type	Range	DOF	Result Datafile 1 (Refer attachments)	Result Datafile2 (Refer attachments)	Scaled numbers*	C.L.^	Result
Instant Games	2	1	Instant_2_Results.2023-06-19-17-04-59.slk	Instant_2_Results.2023-06-20-12-33-32.slk	505000	95%	Pass
Instant Games	8	7	Instant_8_Results.2023-06-19-11-00-56.slk	Instant_8_Results.2023-06-19-12-01-44.slk	505000	95%	Pass
Instant Games	9	8	Instant_9_Results.2023-06-19-11-00-56.slk	Instant_9_Results.2023-06-19-12-01-44.slk	505000	95%	Pass
Instant Games	16	15	Instant_16_Results.2023-06-19-11-00-56.slk	Instant_16_Results.2023-06-19-12-01-44.slk	505000	95%	Pass
Instant Games	25	24	Instant_25_Results.2023-06-19-11-00-56.slk	Instant_25_Results.2023-06-19-17-04-59.slk	505000	95%	Pass
Instant Games	96	95	Instant_96_Results.2023-06-19-11-00-56.slk	Instant_96_Results.2023-06-19-12-01-44.slk	660000	95%	Pass
Keno	1 to 40, drawn 10	390	Keno_40_Results.2023-06-19-11-00-56.slk	Keno_40_Results.2023-06-19-12-01-44.slk	39895000	95%	Pass
Keno	1 to 80, drawn 10	790	Keno_80_Results.2023-06-19-12-01-44.slk	Keno_80_Results.2023-06-19-17-04-59.slk	39895000	95%	Pass
Slot	100000	99999	Reel_100000_results.2023-06-19-11-00-56.slk	Reel_100000_results.2023-06-19-12-01-44.slk	206000000	95%	Pass

Table A.2 Card Games

Game Type	DOF	Result Datafile 1 (Refer attachments)	Result Datafile2 (Refer attachments)	Scaled numbers*	C.L.^	Result
Single Deck (without joker)	Cards/Deal: 52 Suits: 156 Ranks: 624 Cards: 2652	Deck1Joker0_Results.2023-06-19-12-01-44.slk	Deck1Joker0_Results.2023-06-19-17-04-59.slk	77265000	95%	Pass
Two Decks (without joker)	Cards/Deal: 104 Suits: 312 Ranks: 1248 Cards: 5304	Deck2Joker0_Results.2023-06-22-15-10-16.slk	Deck2Joker0_Results.2023-06-22-15-48-01.slk	156045000	95%	Pass

* Scaled numbers for each data file; ^ Confidence Level