



Certification Report: ITL2103205

EPIC88 Limited

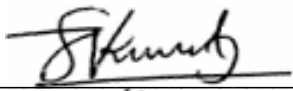
**Random Number Generator Certification Report
Isle of Man Gaming Commission**

11 November 2021

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

Certification Report: ITL2103205

1. Test Laboratory details

N°	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	13 October 2021
4.	Date Completed	11 November 2021
5.	Scope of Work	Certification of the new software RNG for the software provider, EPIC88 Limited
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

N°	Description	Details
1.	Identification	EPIC88 Limited RNG
2.	Type of system:	Online Casino
3.	Games using this RNG:	Non-card games: Slots game
4.	Jurisdiction	Isle of Man
5.	Guidelines used for testing	Isle of Man Technical Standards – The Online Gambling (Systems Verification) (No. 2) Regulations 2007 - Statutory Document No. 731/07
6.	Software provider	Name: EPIC88 Limited Address: 56, Innovation Centre, Level 1, Tower Street, Swatar, Birkirkara BKR 4011, Malta URL: http://avatarux.com Contact: Krzysztof Opalka Email: krzysztof.opalka@gmail.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

N°	Description	Details
1.	RNG type	Pseudo Random Number Generator (PRNG)
2.	Implementation language	JavaScript
3.	RNG version number	1.0.0
4.	RNG build number	1.0.0
5.	Superseded RNG	The RNG has not been previously certified.

Certification Report: ITL2103205

N°	Description	Details
6.	RNG algorithm	ISAAC
7.	Period of algorithm	There are no cycles in ISAAC shorter than 2^{40} values and the expected cycle length is 2^{8295} values.
8.	Dimension of numbers from algorithm	32-bit integer with the interval 0 to $(2^{32}-1)$.
9.	Seeding	Seeding is done from combination of the entropy listed below: current process ID and Math.Random(), a nodejs library implementation, which uses /dev/urandom. /dev/urandom gathers environmental noise from device drivers and other sources into an entropy pool. It also keeps an estimate of the number of bits of noise in the entropy pool.
10.	Reseeding	No Reseeding
11.	Library name and version	None
12.	Operating system	Linux
13.	Environmental particulars	Platform supplier hosting the RNG: N/A Platform version hosting the RNG: N/A
14.	Files and SHA-1 hashes	Refer to Section 2.3 Critical Components of RNG Table 1 and Table 2 below for the list 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
isaac.js	8,585	06e1860835984ee3415398c3b2ba7f17a2e224dd

Table 2: SHA-1 Signature of executables

File Name	Size (bytes)	SHA-1
isaac.js	8,585	06e1860835984ee3415398c3b2ba7f17a2e224dd

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 Slots game.
4.	Statistical tests	The statistical tests undertaken by iTech Labs are: a) Diehard tests b) Chi-square tests

Certification Report: ITL2103205

Nº	Description	Details
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) i. Wikipedia: https://en.wikipedia.org/wiki/ISAAC_(cipher)/

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	No
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 xi. MINIMUM DISTANCE TEST xii. THE 3DSPHERES TEST xiii. THE SQUEEZE TEST xiv. OVERLAPPING SUMS TEST xv. RUNS TEST xvi. CRAPS TEST	Comply Refer Section 4.1 for results.
5.	Statistical testing of scaled / shuffled data	Chi-square tests were conducted for the following: DOF for Slots (Range = 2): 1 DOF for Slots (Range = 4): 3 DOF for Slots (Range = 5): 4	Comply Refer Section 4.2 for results

Certification Report: ITL2103205

Nº	Test Performed	Test Methodology	Result
		DOF for Slots (Range = 6): 5 DOF for Slots (Range = 8): 7 DOF for Slots (Range = 9): 8 DOF for Slots (Range = 15): 14 DOF for Slots (Range = 16): 15 DOF for Slots (Range = 17): 16 DOF for Slots (Range = 18): 17 DOF for Slots (Range = 19): 18 DOF for Slots (Range = 20): 19 DOF for Slots (Range = 21): 20 DOF for Slots (Range = 22): 21 DOF for Slots (Range = 23): 22 DOF for Slots (Range = 24): 23 DOF for Slots (Range = 25): 24 DOF for Slots (Range = 26): 25	
6.	Other	The above test results apply to the code provided by the customer as specified in section 2.3.	-

3.2 Compliance to technical standards

Nº	Requirement Description	Results	Comments
Schedule 1 Randomness			
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	
	(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 and hardware generating the sequence, and all previously generated numbers;	Comply	
	(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	
4.	The Operator must disclose the methodology of any random seeding and any seeding must be proven to result in an unpredictable output.	Comply	

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



Certification Report: ITL2103205

Result Random sequence-1	Result Random sequence-2	Sample size	Confidence level	Result
Refer to attachment CloudTech1.txt	Refer to attachment CloudTech2.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	None
2.	Certification	Certification Date: 11 November 2021 Software Provider: EPIC88 Limited Software Provider site URL: http://avatarux.com Operator Name: N/A Operator site URL: N/A iTech Labs certifies that the Random Number Generator (RNG) as specified in Section 2.3 of this report and used by EPIC88 Limited, complies with the Isle of Man Technical Standards – The Online Gambling (Systems Verification) (No. 2) Regulations 2007 - Statutory Document No. 731/07. iTech Labs recommends that the Random Number Generator (RNG) specified in Section 2.3 of this report be approved for deployment, subject to the conditions listed in Section 5. Final declaration and conformity Item 1.

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
11 November 2021

Kiren Sreekumar
Principal Consultant
iTech Labs
11 November 2021



Certification Report: ITL2103205

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

Non Card Games

Game Type	Range	DOF	Result Datafile 1 (Refer attachments)	Result Datafile2 (Refer attachments)	Scaled numbers*	C.L.^	Result
Slots	2	1	Reel_2_Results.2021-11-01-10-27-28.slk	Reel_2_Results.2021-11-01-12-33-35.slk	505000	95%	Pass
	4	3	Reel_4_Results.2021-11-01-10-25-04.slk	Reel_4_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	5	4	Reel_5_Results.2021-11-01-10-25-04.slk	Reel_5_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	6	5	Reel_6_Results.2021-11-01-10-25-04.slk	Reel_6_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	8	7	Reel_8_Results.2021-11-01-10-25-04.slk	Reel_8_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	9	8	Reel_9_Results.2021-11-01-10-25-04.slk	Reel_9_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	15	14	Reel_15_Results.2021-11-01-10-25-04.slk	Reel_15_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	16	15	Reel_16_Results.2021-11-01-10-25-04.slk	Reel_16_Results.2021-11-01-10-27-28.slk	505000	95%	Pass
	17	16	Reel_17_Results.2021-11-01-10-25-04.slk	Reel_17_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	18	17	Reel_18_Results.2021-11-01-10-25-04.slk	Reel_18_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	19	18	Reel_19_Results.2021-11-01-10-25-04.slk	Reel_19_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	20	19	Reel_20_Results.2021-11-01-10-25-04.slk	Reel_20_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	21	20	Reel_21_Results.2021-11-01-10-25-04.slk	Reel_21_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	22	21	Reel_22_Results.2021-11-01-10-25-04.slk	Reel_22_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	23	22	Reel_23_Results.2021-11-01-10-25-04.slk	Reel_23_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	24	23	Reel_24_Results.2021-11-01-10-25-04.slk	Reel_24_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	25	24	Reel_25_Results.2021-11-01-10-25-04.slk	Reel_25_Results.2021-11-01-10-26-39.slk	505000	95%	Pass
	26	25	Reel_26_Results.2021-11-01-10-25-04.slk	Reel_26_Results.2021-11-01-10-26-39.slk	505000	95%	Pass

* Scaled numbers for each data file; ^ Confidence Level