Certification Report: ITL2101701

Jumbo Interactive T/as Benon Technologies

Random Number Generator Certification Report
UK Gaming Commission

29 June 2021

NATA WORLD RECOGNISED ACCREDITATION	iTech Labs is accredited for compliance with ISO/IEC 17025 – Testing and ISO/IEC 17020. NATA is a signatory to the ILAC Mutual Recognition Arrangement for the mutual recognition of the equivalence of testing and inspection. Accreditation number: 15690 *Links for scope of accreditation: ISO/IEC 17025 and ISO/IEC 17020*

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

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	27 May 2021
4.	Date Completed	29 June 2021
5.	Scope of Work	Certification of the new software RNG for the software provider, Jumbo Interactive T/as Benon technologies.
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	Jumbo Interactive T/as Benon technologies RNG
2.	Type of system	Online Casino
3.	Games using this RNG	Non-card games: Raffle game
4.	Jurisdiction	UK
5.	Guidelines used for testing	UK Remote Gambling and Software Technical Standards February 2021 Testing Strategy for Compliance with Remote Gambling and Software Technical Standards February 2021.
6.	Software provider	Name: Jumbo Interactive T/as Benon technologies Address: P.O. Box 824, Toowong Queensland, Australia URL: https://www.jumbointeractive.com/ Contact: James Hume Email: jamesh@benon.com
7.	Operator details	Operator Name: St. Helena Hospice Address: 6 The Atrium, Phoenix Square, Colchester, Essex, C04 9AS URL:www.makeasmilelottery.org.uk; www.yourhospicelottery.org.uk Contact: Gemma Zweck Email: gemma@yhlhospices.org.uk

2.2 Description of RNG

2.2.1 Software Details

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

Nº	Description	Details
3.	RNG version number	v1.1
4.	RNG build number	git hash for RNG (not drawmaster) - 8dd3c313fe57b27bbba5c40ce70c8aa5c2ac3639
5.	Superseded RNG	The RNG has not been previously certified.
6.	RNG algorithm	Linux /dev/urandom which uses system entropy and ChaCha20 algorithm with continuous injection of entropy as and when available.
7.	Period of algorithm	Indeterminate (There is no period because of entropy being mixed into the states when available).
8.	Dimension of numbers from algorithm	8 bits (Data available is read out in chunks of bytes - not integers - 4 consecutive bytes are combined to obtain a 32-bit number prior to scaling).
9.	Seeding	Seeded by the Operating system at start up using System entropy.
10.	Reseeding	Reseeding performed automatically as and when adequate entropy becomes available.
11.	Library name and version	This RNG uses Golang library "crypto/rand" function which in turn draws numbers from the Linux Operating system RNG /dev/urandom. Hence the RNG certification is restricted to GO library versions 1.0 to 1.16.x(current) and Linux Kernel versions 4.9.x to 5.12.x (current).
12.	Operating system	Linux
13.	Environmental particulars	Platform supplier hosting the RNG: AWS - Fargate 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
rng/internal/handler/urandom/urandom.go	1,695	70503112e84ab8d799af1d2b40a66d2e0bdf80e3

Table 2: SHA-1 Signature of executables

File Name	Size (bytes)	SHA-1
rng	4,796,416	fadfd0b2a76d34280a7cb26df9ed03d18a6b122d

2.4 Scope of Testing

Nº	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. Refer to Section 2.3 Critical Components of RNG.

Nº	Description	Details
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 Raffle game.
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) https://www.2uo.de/myths-about-urandom/ http://eprint.iacr.org/2012/251.pdf https://cr.yp.to/chacha/chacha-20080128.pdf https://en.wikipedia.org/wiki//dev/random

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	This RNG uses Golang library function RNG "crypto/rand" which in turn draws numbers from the Linux Operating system RNG /dev/urandom. Hence the RNG certification is restricted to Linux Kernel versions 4.9.x to 5.12.x (current).
3.	Library-based implementation	This RNG uses Golang library function "crypto/rand". Hence the RNG certification is restricted to GO library versions 1.0 to 1.16.x(current).
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	Comply Refer Section 4.1 for results.

Nº	Test Performed	Test Methodology	Result
		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	
5.	Statistical testing of scaled / shuffled data	Chi-square tests were conducted for the following: DOF for Raffle game (Range = 2) = 1 DOF for Raffle game (Range = 15) = 14 DOF for Raffle game (Range = 128) = 127 DOF for Raffle game (Range = 1025) = 1024 DOF for Raffle game (Range = 10000) = 9999 DOF for Raffle game (Range = 262145) = 198, 316, 442, 508, 999 DOF for Raffle game (Range = 4194303) = 198, 316, 442, 508, 999 DOF for Raffle game (Range = 10000000) = 198, 316, 442, 508, 999 Note: The tests for ranges 262145, 4194303 and 10000000 were run by dividing the range into a specified number of equal sized buckets and testing for uniformity in distribution of numbers that fall in each bucket. Each range test was run with 5 different bucket counts - the first being 1000 buckets (range divided into 1000 equal buckets) and the other 4 being arbitrary prime numbers - 199, 317, 443 and 509 buckets.	Comply Refer Section 4.2 for results
6.	Other issues	None	-

3.2 Compliance to technical standards

Nº	Requirement Description	Results	Comments
RTS 7A	Random number generation and game results must be 'acceptably random'. Acceptably random here means that it is possible to demonstrate to a high degree of confidence that the output of the RNG, game, lottery and virtual event outcomes are random, through, for example, statistical analysis using generally accepted tests and methods of analysis. Adaptive behaviour (i.e. a compensated game) is not permitted. Where lotteries use the outcome of other events external to the lottery, to determine the result of the lottery (for example, using numbers from the National Lottery) the outcome must be unpredictable and externally verifiable.	Comply	RNG complies for all requirements for the game types listed in Section 2.1 General Information, Item 3. Note: The requirements that are also influenced by game logic, must be covered by separate game certification.
RTS 7B	As far as is reasonably possible, games and events must be implemented fairly and in accordance with the rules and	Comply	RNG complies for all requirements for the game types listed in Section 2.1 General Information, Item 3.

Nº	Requirement Description	Results	Comments
	prevailing payouts, where applicable, as they are described to the customer.		Note: The requirements that are also influenced by game logic, must be covered by separate game certification.

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 Jumbo1.txt	Refer to attachment Jumbo2.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 GO library versions 1.0 to 1.16.x (current) and Linux Kernel versions 4.9.x to 5.12.x (current).
2.	Certification	Certification Date: 29 June 2021 Software Provider: Jumbo Interactive T/as Benon Technologies Software Provider site URL: https://www.jumbointeractive.com Operator Name: St. Helena Hospice Operator site URL: www.makeasmilelottery.org.uk; www.yourhospicelottery.org.uk iTech Labs certifies that the Random Number Generator (RNG) as specified in Section 2.3 of this report and used by Jumbo Interactive T/as Benon Technologies, complies with the UK Remote Gambling and Software Technical Standards February 2021 and the Testing Strategy for Compliance with Remote Gambling and Software Technical Standards February 2021. 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:	
Signed by: **Geoff Nicoll** Principal Consultant **iTech Labs** 29 June 2021	Authorised by: **Kiren Sreekumar** Principal Consultant **iTech Labs** 29 June 2021

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
Raffle game	2	1	single-2-results-20210615103836.xls	single-2-results-20210615104510.xls	3400000	95%	Pass
	15	14	single-15-results-20210615103757.xls	single-15-results-20210615104432.xls	3400000	95%	Pass
	128	127	single-128-results-20210615103332.xls	single-128-results-20210615104008.xls	3400000	95%	Pass
	1025	1024	single-1025-results-20210615103254.xls	single-1025-results-20210615103929.xls	4800000	95%	Pass
	10000	9999	single-10000-results-20210615103348.xls	single-10000-results-20210615104024.xls	34000000	95%	Pass
	262145	198, 316, 442, 508, 999	single-262145-results-20210615103730.xls	single-262145-results-20210615104406.xls	17000000	95%	Pass
	4194303	198, 316, 442, 508, 999	single-4194303-results-20210615104351.xls	single-4194303-results-20210615105458.xls	17000000	95%	Pass
	10000000	198, 316, 442, 508, 999	single-10000000-results-20210615104448.xls	single-10000000-results-20210615105556.xls	17000000	95%	Pass

** Scaled numbers for each data file; ^ Confidence Level*