Certification Report: ITL2002937

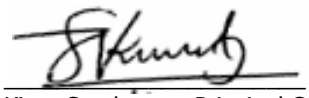
NetEnt Product Services Ltd

Random Number Generator Certification Report
Malta Gaming Authority

11 December 2020

Certification Report: ITL2002937

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	16 November 2020
4.	Date Completed	11 December 2020
5.	Scope of Work	Re-certification of the software RNG for the software provider, NetEnt Product Services Ltd This is a recertification of the NetEnt RNG which has been previously certified by iTech Labs. iTech Labs has conducted evaluation of the RNG by comparing the new source code of the RNG to the previously approved RNG to identify any changes. There were no changes to the functionality of the NetEnt RNG.
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	NetEnt Product Services Ltd RNG
2.	Type of system:	Online Casino
3.	Games using this RNG:	Non-card games: Roulette (Ameican Roulette, European Roulette) Scratch Ticket Slots Card games: eight decks without joker six decks without joker four decks without joker single deck without joker single deck with joker
4.	Jurisdiction	Malta Gaming Authority
5.	Guidelines used for testing	Malta Remote Gaming Regulations 2004 S.L.438.04.
6.	Software provider	Name: NetEnt Product Services Ltd Address: Level One, Spinola Park, Mikiel Ang. Borg Street SPK1000 St. Julians, Malta URL: www.netent.com Contact: Anna-Karin Silver Email: anna-karin.silver@netent.com
7.	Operator details	Not Applicable

2.2 Description of RNG

2.2.1 Software Details

Nº	Description	Details
1.	RNG type:	Pseudo Random Number Generator (PRNG)
2.	Implementation language	Java
3.	RNG version number:	1.0
4.	RNG build number:	1.0
5.	Superseded RNG:	This is a recertification of the NetEnt RNG which has been previously certified for Malta.
6.	RNG algorithm	Fortuna
7.	Period of algorithm	Indeterminate (not expected to repeat due to the continuous addition of entropy into the system).
8.	Dimension of numbers from algorithm	32 bit (0 to 2^32-1)
9.	Seeding	Seeding is from Entropy Sources.
10.	Reseeding	The algorithm is based on continuous reseeding from multiple entropy sources (This has been assessed and found acceptable).
11.	Library name and version	Not Applicable
12.	Operating system	Windows
13.	Environmental particulars	Platform supplier hosting the RNG: Not Applicable Platform version hosting the RNG: Not Applicable
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
random.fortuna.entropy.source.DevUrandomEntropySource.java	1,221	b14084dbfc81231f1654d2c40051cc749fd78eef
random.fortuna.entropy.source.DiskWriteEntropySource.java	1,674	fee592453e728f0d036d5e239a4b9ee215be4544
random.fortuna.entropy.EntropyAccumulator.java	3,929	f3771dfcb2d8395df697cbfa2b96e726804158dc
random.fortuna.entropy.EntropyBytes.java	1,322	db822b0f4969a25143779f358cd70d86ed359ac2
random.fortuna.entropy.EntropyCollector.java	950	d9e6377138da3e48f824b6e06e3582177f66c5f7
random.fortuna.entropy.EntropyPool.java	2,983	8a5b6de1ba26dd4776fd2d7a745028ac484c3a31
random.fortuna.entropy.source.EntropySource.java	214	a617158a242af326a7095bfb079fcad9bd1346c5
random.fortuna.FortunaGenerator.java	3,427	d93ccee29c026b5b517e577c656fee7c6fe4c25e
random.fortuna.FortunaRandom.java	5,387	7e41f165f2da988960723792d89c024b351ef63f
random.fortuna.entropy.source.GarbageCollectionTimeEntropySource.java	741	51a3dbfe66052611c01522df23e6e32ada7837bc
random.fortuna.entropy.source.HeapMemoryEntropySource.java	671	2dc94da5daa0ccb398dc3c30914ddd6ccfea6e36
random.fortuna.entropy.source.LoadAverageEntropySource.java	778	d5919b7c73c52c31fbf495e474d93bc6c0f27e48
random.fortuna.entropy.source.ObjectsPendingFinalizationEntropySource.java	694	7de3043ed141a87331ad11b258b54a48950b0695
common.commonservice.service.random.RandomGeneratorImpl.java	1,345	cb6ed13f22e465983b9f330f82fc3750ee0f8b0d
common.commonservice.service.random.RandomNumberGenerator.java	6,487	fdb5b074de173868c52f2da09702d792a27eaa4f
random.fortuna.seed.SecureRandomSeedGenerator.java	591	c20a552d6cb2aa0cd9e2ce3fb261ff0d447d0408
random.fortuna.seed.SeedGeneratorFactory.java	298	e1dd1db84b62e683b69b1f29b68f4f806c115de1
random.fortuna.seed.SeedGenerator.java	120	049ff5469c58d74c7049f187e43dc942098b79c9
random.fortuna.entropy.source.ThreadCpuTimeEntropySource.java	756	128c645417d3732c8528bc302ff2a65fd2edfb17
random.fortuna.entropy.source.ThreadSchedulerEntropySource.java	892	8d5873f64312302a9987ac26c5f14c9e7ae83e33
random.fortuna.seed.UnixSeedGenerator.java	635	b283816dbf6d7a50aac75db13d6514d428cfc8a1
random.fortuna.entropy.source.UptimeEntropySource.java	859	7d32c83a2a93f8ff3883f1ca50f26a913fe3bf91
random.fortuna.entropy.source.UsedJvmMemoryEntropySource.java	717	f990ec23d42539464f96735f39d407a3c4da162d

Table 2: SHA-1 Signature of executables

File Name	Size (bytes)	SHA-1
spp-rng-wrapper-1.0.0.jar	4,988	825411cce989542b305c586c86c00166a7ed6bae
fortuna-1.0.jar	24,633	b95bf8a83025f2175e4c3ecd040cc12e3d58f349

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.
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 non-card games; d) Shuffling for card 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) i. Wikipedia: https://en.wikipedia.org/wiki/Fortuna_%28PRNG%29

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	None
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 RNG algorithm to ensure there is no publicly known weakness or vulnerabilities associated 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	Comply Refer Section 4.1 for results.

Nº	Test Performed	Test Methodology	Result
		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 SQEEZE 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 European Roulette (Range= 0 to 36): 36 • DOF for American Roulette (Range= 0 to 37): 37 • DOF for Slots (Range= 0 to 1): 1 • DOF for Slots (Range= 0 to 31): 31 • DOF for Slots (Range= 0 to 32): 32 • DOF for Slots (Range= 0 to 62): 62 • DOF for Slots (Range= 0 to 63): 63 • DOF for Slots (Range= 0 to 64): 64 • DOF for Slots (Range= 0 to 999): 999 • DOF for Slots (Range= 0 to 9999): 9999 • DOF for Sratch ticket games (Range= 0 to 1,000,000): 198, 316, 442, 508 and 999 • DOF for Sratch ticket games (Range= 0 to 2,000,000): 198, 316, 442, 508 and 999 • DOF for eight decks (without joker): Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304 • DOF for six decks (without joker): Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304 • DOF for six decks (without joker): Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304 • DOF for four decks (without joker): Card/deal: 104 Suit: 312 Rank: 1248	Comply Refer Section 4.2 for results

Nº	Test Performed	Test Methodology	Result
		Card: 5304 • DOF for single deck (without joker): Card/deal: 52 Suit: 156 Rank: 624 Card: 2652 • DOF for single deck (with joker): Card/deal: 53 Suit: 212 Rank: 689 Card: 2756	
6.	Other issues	None	-

3.2 Compliance to technical standards

Nº	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	

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 Fortuna1.txt	Refer to attachment Fortuna2.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 December 2020 Software Provider: NetEnt Product Services Ltd Software Provider site URL: www.netent.com Operator Name: Not Applicable Operator site URL: Not Applicable This is to certify that iTech Labs has evaluated the Random Number Generator (RNG) by NetEnt Product Services Ltd and found that the RNG complies with the relevant standards and is in conformity to the Malta Remote Gaming Regulations S.L.438.04. 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.

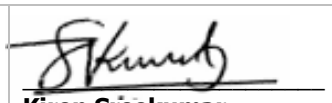
6 Conclusion

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 December 2020



Kiren Sreekumar
Principal Consultant
iTech Labs
11 December 2020

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

Table A.1 Card Games

Game Type	DOF	For result for Data File 1 and Data File 2 (See the following attachments)	Scaled numbers in each data file	Confidence level	Result
Single deck without joker (Shuffle 2)	Card/deal: 52 Suit: 156 Rank: 624 Card: 2652	results-1deck-2-20161201133921.xls, results-1deck-2-20161201133950.xls	950000	95%	Passed
Single deck with one joker (Shuffle 2)	Card/deal: 53 Suit: 212 Rank: 689 Card: 2756	results-1deck-1joker-2-20161201131816.xls, results-1deck-1joker-2-20161201132522.xls	950000	95%	Passed
Single deck without joker	Card/deal: 52 Suit: 156 Rank: 624 Card: 2652	results-1deck-20161201130329.xls, results-1deck-20161201130421.xls	950000	95%	Passed
Four decks without joker (Shuffle 2)	Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304	results-4deck-2-20161201134957.xls, results-4deck-2-20161201135227.xls	950000	95%	Passed
Four decks without joker	Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304	results-4deck-20161201134347.xls, results-4deck-20161201134427.xls	950000	95%	Passed
Six decks without joker (Shuffle 2)	Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304	results-6deck-2-20161201145540.xls, results-6deck-2-20161201150730.xls	950000	95%	Passed
Eight decks without joker (Shuffle 2)	Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304	results-8deck-2-20161201152220.xls, results-8deck-2-20161201154801.xls	950000	95%	Passed
Eight decks without joker	Card/deal: 104 Suit: 312 Rank: 1248 Card: 5304	results-8deck-20161201152136.xls, results-8deck-20161201154804.xls	950000	95%	Passed

Table A.2 Non Card Games

Game Type	Range	DOF	For result for Data File 1 and Data File 2 (See the following attachments)	Scaled numbers in each data file	Confidence level	Result
Slot	0 to 1	1	single-0-1-results-20161201160931.xls, single-0-1-results-20161201161508.xls	18880000	95%	Passed
Slot	0 to 31	31	single-0-31-results-20161201163501.xls, single-0-31-results-20161202124504.xls	18880000	95%	Passed
Slot	0 to 32	32	single-0-32-results-20161202125504.xls, single-0-32-results-20161202125532.xls	18880000	95%	Passed
Slot	0 to 62	62	single-0-62-results-20161202130516.xls, single-0-62-results-20161202130548.xls	18880000	95%	Passed
Slot	0 to 63	63	single-0-63-results-20161202131323.xls, single-0-63-results-20161202131407.xls	18880000	95%	Passed
Slot	0 to 64	64	single-0-64-results-20161202132242.xls, single-0-64-results-20161202132555.xls	18880000	95%	Passed
Slot	0 to 999	999	single-0-999-results-20161202133511.xls, single-0-999-results-20161202133557.xls	19100000	95%	Passed
Slot	0 to 9999	9999	single-0-9999-results-20161202134145.xls, single-0-9999-results-20161202134250.xls	24000000	95%	Passed
European Roulette	0 to 36	36	single-0-36-results-20161202130006.xls, single-0-36-results-20161202130036.xls	18880000	95%	Passed
American Roulette	0 to 37	37	single-0-37-results-20191127145717.xls, single-0-37-results-20191127145620.xls	18880000	95%	Passed
Scratch	0 to 1,000,000	198, 316, 442, 508 and 999	single-1000000-results-20161202134920.xls single-1000000-results-20161202135534.xls	111000000	95%	Passed
Scratch	0 to 2,000,000	198, 316, 442, 508 and 999	single-2000000-results-20161202140553.xls single-2000000-results-20161202140635.xls	211000000	95%	Passed