Random Number Generator Evaluation Report for Yggdrasil Gaming Ltd

20 May 2020

Certification number: ITL2001215

1. Test Laboratory Details

iTech Labs URL: http://www.itechlabs.com

Suite 24, 40 Montclair Ave e-mail: info@itechlabs.com
Glen Waverley
VIC 3150, Australia

iTech Labs is accredited to ISO/IEC 17025 and ISO/IEC 17020 by National Association of Testing Authorities (NATA), to undertake compliance testing and audits of online gaming systems. iTech Labs scope of accreditation (#15690) can be downloaded from NATA website www.nata.com.au. NATA is a member of the International Laboratories Association Co-operation Mutual Recognition Agreement (ILAC MRA).

All assessments in the following sections of this report are provided under ISO/IEC 17025 and/or ISO/IEC 17020 except where otherwise stated.

Links for scope of accreditation: ISO/IEC 17025 and ISO/IEC 17020

Location(s) where testing was performed: as above

Date Commenced: 15 May 2020

Date Completed: 20 May 2020

Certificate reference number: ITL2001215

Test supervisor signature:

2. Executive Summary

i) Introduction

Software Provider details:

Yggdrasil Gaming Ltd is a software provider for online gaming systems. This RNG is developed by Yggdrasil Gaming Ltd for use in Slot, Roulette and Card games.

Yggdrasil Gaming Ltd URL: www.yggdrasilgaming.com

Tagliaferro Business Centre, Level 2
High Street c/w Gaiety Lane
Sliema, SLM 1551, Malta

To: Andrii Grygorovych e-mail: andrii@yggdrasilgaming.com

System: Online games

Games using this RNG: Slot, Roulette and Card games

Jurisdictions: UK

Applicable standards: UK Remote Gambling and Software Technical Standards - June 2017

Licensee details:

Licensee Name: Yggdrasil Gaming Ltd

Licensee address: Tagliaferro Business Centre, Level 2 High Street c/w Gaiety Lane Sliema, SLM 1551, Malta
Licensee contact information: andrii@yggdrasilgaming.com
Platform supplier name: Yggdrasil Gaming Ltd
Platform version: 2.48

ii) Description of RNG

Yggdrasil Gaming Ltd RNG is a Pseudo Random Number Generator (PRNG). It is implemented in Java language.

RNG algorithm: Mix of Mersenne Twister algorithm and SHA1PRNG Secure Random.

Period of MT: (2^19937 – 1)

Period of SHA1PRNG: 2^160

Dimension of numbers from MT: 32 bit integer with the interval 0 to (2^32-1).

Dimension of numbers from SHA1PRNG: 32 bit integer with the interval 0 to (2^32-1).

Seeding: Seeded with the output of a SecureRandom which is in turn auto seeded by system entropy source.

Reseeding: Reseeding provision exists – done infrequently at about once per day.

Games utilising the RNG: Slot, Roulette and card games

iii) Scope of Testing

Previous history of testing this RNG: This RNG was previously certified for slots, roulette and card games.
This is a re-certification due to changes in the checksums of critical binaries which is due to the effect of dependencies involved in compilation. There is no change to the actual critical source (.java) files.

1. Vendor supplied output testing: Not Applicable (not used)
2. Tester generated output from vendor supplied source: Yes. The source files were compiled by iTech Labs

   Hash of source files: See Appendix-A.1

   Hash of executable files: See Appendix-A.2

   Operational environment:

   a) Operating system: Linux
   b) Source code language: Java
   c) Library name and version (if library based RNG): N/A
   d) Build number: 2.48
3. Source code review: The following source code evaluation was conducted:
   a) Identification of algorithm
   b) Security of internal state, seeding and re-seeding, thread safety
   c) Scaling for slot and roulette games and shuffling for card games
4. Theoretical basis of algorithm and supporting crypto-analysis evidence:

   RNG Algorithm used is Mix of Mersenne Twister algorithm and SHA1PRNG Secure Random. Literature is readily available, describing the theoretical basis of the algorithm.

   e.g.,
   Mersenne Twister (the original site of the authors):

http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html

SHA1PRNG:
http://docs.oracle.com/javase/1.5.0/docs/guide/security/CryptoSpec.html#AppA

Wikipedia:

http://en.wikipedia.org/wiki/Mersenne_twister

http://es.wikipedia.org/wiki/SHA1PRNG

5. Limitations of assurance because of scope of testing (range, degrees of freedom, seeding, re-starting, etc) likely foreseen by tester

The only limitations of assurance are listed below under "iv) Limitations of use of RNG".

iv) Limitations of use of RNG

The following Limitations of use of RNG was applied for previous certification:

1. The acceptable degrees of freedom (DOF)

DOF for slot games with multiple ranges:

52, 62, 64, 68, 75, 87, 93, 127, 193

DOF for single number range 5 : 4

DOF for single number range 37 : 36

DOF for single number range 10000 : 9999

DOF for single number range 100000 : 99999

DOF for shuffle range 1 to 7 : 42

DOF for shuffle range 1 to 9 :72

DOF for shuffle range 1 to 10 : 90

DOF for shuffle range 1 to 11: 110

DOF for shuffle range 1 to 15: 210

DOF for shuffle range 1 to 40: 1560

DOF for shuffle range 1 to 52: 2652

DOF for shuffle range 1 to 53: 2756

DOF for shuffle range 1 to 80: 6320

DOF for shuffle range 0 to 158: 25122

DOF for shuffle range 0 to 206: 42642

DOF for shuffle range 0 to 227: 51756

DOF for shuffle range 0 to 263: 69432

DOF for shuffle range 0 to 281: 79242

DOF for shuffle range 0 to 581: 338142

DOF for roulette games with multiple ranges:

DOF for European Roulette (Range - 37) : 36

DOF for Weighted Single Number (Weights=320,90,300,88,10,2,1) : 6

DOF for one deck (with no joker):

Cards/Deal: 52

Tests	DOF
Suits	156
Ranks	624
Cards	2652

DOF for one deck (with one joker):

Cards/Deal: 53

Tests	DOF
Suits	212
Ranks	689
Cards	2756

DOF for six deck (with no joker):

Cards/Deal: 312

Tests	DOF
Suits	936
Ranks	3744
Cards	15912

2. Any dependency on operating system functionality that if modified could impact on the operation of the RNG (e.g. Java SecureRandom)

   None

3. Limitation due to library based implementation

   N/A

v) Certification

RNG complies with requirements as listed in 3.2 of this report, subject to:
None

Certification according to UK Gambling commission standards

Certification for Software provider
iTech Labs certifies that the Random Number Generator (RNG) specified in Appendix-A and used by Yggdrasil Gaming Ltd complies with UKGC 'Red' category testing requirements according to UK Remote Gambling and Software Technical Standards – June 2017, and Testing strategy for compliance with remote gambling and software technical standards, November 2018.

iTech Labs recommends that the Random Number Generator (RNG) specified in Appendix-A and be approved for deployment, subject to the above.

3. Detailed test results

3.1 Test methodology

This RNG was previously certified for slots, roulette and card games.

This is a re-certification due to changes in the checksums of critical binaries which is due to the effect of dependencies involved in compilation. There is no change to the actual critical source (.java) files.

The following test methodology was applied for previous certification:

1. Review of RNG documentation

   Review of RNG documentation was conducted to understand the implementation of RNG in the gaming system.

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.

3. Review of source code

   Review of source code was conducted to verify the implementation of RNG is in accordance with the RNG documentation.
   The source code review included the following:

   a) Identification of algorithm
   b) Security of internal state, seeding and re-seeding, thread safety
   c) Scaling for slot and roulette games
   d) Shuffling for card games

4. Statistical testing of raw output of RNG and scaled/shuffled decks data.

   a) 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 SQEEZE test
      xiv) OVERLAPPING SUMS TEST
      xv) RUNS TEST
      xvi) CRAPS TEST

   b) Chi-square tests were conducted for the following:

      DOF for slot games with multiple ranges:

      52, 62, 64, 68, 75, 87, 93, 127, 193

      DOF for single number range 5 : 4

      DOF for single number range 37 : 36

DOF for single number range 10000 : 9999

DOF for single number range 100000 : 99999

DOF for shuffle range 1 to 7 : 42

DOF for shuffle range 1 to 9 :72

DOF for shuffle range 1 to 10 : 90

DOF for shuffle range 1 to 11: 110

DOF for shuffle range 1 to 15: 210

DOF for shuffle range 1 to 40: 1560

DOF for shuffle range 1 to 52: 2652

DOF for shuffle range 1 to 53: 2756

DOF for shuffle range 1 to 80: 6320

DOF for shuffle range 0 to 158: 25122

DOF for shuffle range 0 to 206: 42642

DOF for shuffle range 0 to 227: 51756

DOF for shuffle range 0 to 263: 69432

DOF for shuffle range 0 to 281: 79242

DOF for shuffle range 0 to 581: 338142

DOF for roulette games with multiple ranges:

DOF for European Roulette (Range - 37) : 36

DOF for Weighted Single Number (Weights=320,90,300,88,10,2,1) : 6

DOF for one deck (with no joker):

Cards/Deal: 52

Tests	DOF
Suits	156
Ranks	624
Cards	2652

DOF for one deck (with one joker):

Cards/Deal: 53

Tests	DOF
Suits	212
Ranks	689
Cards	2756

DOF for six deck (with no joker):

Cards/Deal: 312

Tests	DOF
Suits	936
Ranks	3744
Cards	15912

5. Issues resolution

No issues reported during this round of RNG certification.

The following test methodology was applied for this round of recertification:

1. Review of source code

   The source code review was conducted and changes have been evaluated.
   No additional tests were required to be conducted.

2. Issues resolution

   No issues were reported.

3.2 Compliance to requirements

Req No.	Requirement Description	Compliance Status	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 games listed in Appendix-B 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 prevailing payouts, where applicable, as they are described to the customer.	Comply	RNG complies for all requirements for the games listed in Appendix-B Note: The requirements that are also influenced by game logic, must be covered by separate game certification.

3.3 Identification of the RNG

3.3.1 Hardware RNG

Manufacturer: N/A

Model: N/A

Serial number: N/A

Interface type (USB, serial): N/A

Number of modules and configuration: automatic failover, manually switch to backup module, concurrent use of multiple modules: N/A

URL of manufacturer's website for this module: N/A

3.3.2 Software RNG

Supplier: Yggdrasil Gaming Ltd

Version details (unique identifier, version number): 2.48

Environment particulars:

Operating system: Linux

RNG Algorithm: Mix of Mersenne Twister and SHA1PRNG Secure Random

Language of implementation (C++, Java, etc.): Java

Files and SHA-1 Hashes: See Appendix-A

List hashes of source code files and binaries (if applicable) of the RNG evaluated: See Appendix-A

For hardware implementation of the RNG, include hashes of the code (drivers, scaling, etc.) used to implement the RNG: N/A

For software RNG, include hashes of the code for RNG algorithm and the code related to RNG algorithm (seeding, background cycling, scaling, etc.): See Appendix-A

RNG Monitoring: The action on failure is to log a SEVERE level message and send a notification message, and the game would be deactivated manually.

3.3.3 References

List of documents used for reference (compliance requirements, literature/URLs for software RNG, URLs for hardware RNG, supplier's documentation, etc.)

Mersenne Twister (the original site of the authors):
http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html

SHA1PRNG:
http://docs.oracle.com/javase/1.5.0/docs/guide/security/CryptoSpec.html#AppA

Java implementation of MT:
http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/VERSIONS/JAVA/java.html

C and C# implementations:
http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html
http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/VERSIONS/C-LANG/c-lang.html

Wikipedia:
http://en.wikipedia.org/wiki/Mersenne_twister

http://es.wikipedia.org/wiki/SHA1PRNG

4. Statistical testing results

4.1 Testing results for raw output of RNG

Diehard tests

Result for Random sequence-1	Result for Random sequance-2	Sample size	Confidence level	Result
Please see attachment yggdrasil1.txt	Please see attachment yggdrasil2.txt	80 million bits	95%	Passed

Overall result: Diehard tests passed

4.2 Testing results for scaled output of RNG

Confidence level for the tests below: 95%

DOF	Result for Data file 1 (See the following attachments)	Result for Datafile2 (See the following attachments)	Scaled numbers in each data file	Confidence level	Result

52	Yggdrasil-reel53-results-20190708113824.xls	Yggdrasil-reel53-results-20190708113935.xls	18880000	95%	Passed
62	Yggdrasil-reel63-results-20190708113830.xls	Yggdrasil-reel63-results-20190708114036.xls	18880000	95%	Passed
64	Yggdrasil-reel65-results-20190708103739.xls	Yggdrasil-reel65-results-20190708113943.xls	18880000	95%	Passed
68	Yggdrasil-reel69-results-20190708113948.xls	Yggdrasil-reel69-results-20190708114251.xls	18880000	95%	Passed
75	Yggdrasil-reel76-results-20190708113839.xls	Yggdrasil-reel76-results-20190708114826.xls	18880000	95%	Passed
87	Yggdrasil-reel88-results-20190708115049.xls	Yggdrasil-reel88-results-20190715134947.xls	18880000	95%	Passed
93	Yggdrasil-reel94-results-20190708103753.xls	Yggdrasil-reel94-results-20190708114835.xls	18880000	95%	Passed
127	Yggdrasil-reel128-results-20190708103725.xls	Yggdrasil-reel128-results-20190708113816.xls	18880000	95%	Passed
193	Yggdrasil-reel194-results-20190708103730.xls	Yggdrasil-reel194-results-20190708114415.xls	18880000	95%	Passed
42	Yggdrasil-shuffle-7-results-20190708124744.xls	Yggdrasil-shuffle-7-results-20190708124814.xls	1960000	95%	Passed
72	Yggdrasil-shuffle-9-results-20190708124817.xls	Yggdrasil-shuffle-9-results-20190708125140.xls	1960000	95%	Passed
90	Yggdrasil-shuffle-10-results-20190708103938.xls	Yggdrasil-shuffle-10-results-20190708124729.xls	1960000	95%	Passed
110	Yggdrasil-shuffle-11-results-20190708124734.xls	Yggdrasil-shuffle-11-results-20190708124808.xls	1960000	95%	Passed
210	Yggdrasil-shuffle-15-results-20190708103944.xls	Yggdrasil-shuffle-15-results-20190708124739.xls	1960000	95%	Passed
1560	Yggdrasil-shuffle-40-results-20190708104611.xls	Yggdrasil-shuffle-40-results-20190708132632.xls	1960000	95%	Passed
2652	Yggdrasil-shuffle-52-results-20190708104626.xls	Yggdrasil-shuffle-52-results-20190708132645.xls	1960000	95%	Passed
2756	Yggdrasil-shuffle-53-results-20190708132906.xls	Yggdrasil-shuffle-53-results-20190708133221.xls	1960000	95%	Passed
6320	Yggdrasil-shuffle-80-results-20190708132719.xls	Yggdrasil-shuffle-80-results-20190708132925.xls	1960000	95%	Passed

25122	Yggdrasil-shuffle-158-results-20190708103949.xls	Yggdrasil-shuffle-158-results-20190708132539.xls	1960000	95%	Passed
42642	Yggdrasil-shuffle-206-results-20190708135318.xls	Yggdrasil-shuffle-206-results-20190708140721.xls	1960000	95%	Passed
51756	Yggdrasil-shuffle-227-results-20190708135428.xls	Yggdrasil-shuffle-227-results-20190708140834.xls	1960000	95%	Passed
69432	Yggdrasil-shuffle-263-results-20190708104257.xls	Yggdrasil-shuffle-263-results-20190708135547.xls	1960000	95%	Passed
79242	Yggdrasil-shuffle-281-results-20190708141125.xls	Yggdrasil-shuffle-281-results-20190708142256.xls	1960000	95%	Passed
338142	Yggdrasil-shuffle-581-results-20190708104646.xls	Yggdrasil-shuffle-581-results-20190708142428.xls	1960000	95%	Passed
4	Yggdrasil-single-5-results-20190708103933.xls	Yggdrasil-single-5-results-20190708120521.xls	18880000	95%	Passed
36	Yggdrasil-single-37-results-20190708103928.xls	Yggdrasil-single-37-results-20190708120516.xls	18880000	95%	Passed
9999	Yggdrasil-single-10000-results-20190708103758.xls	Yggdrasil-single-10000-results-20190708120338.xls	44000000	95%	Passed
99999	Yggdrasil-single-100000-results-20190708103811.xls	Yggdrasil-single-100000-results-20190708121053.xls	185000000	95%	Passed
36	Yggdrasil-single-37-results-20191219103727.xls	Yggdrasil-single-37-results-20191219104204.xls	18880000	95%	Passed
6	results-weighted-20191219104216.xls	results-weighted-20191219104428.xls	39000000	95%	Passed
212 689 2756	results-cards-1deck-1joker-20190708103440.xls	results-cards-1deck-1joker-20190708111740.xls	740000	95%	Passed
156 624 2652	results-cards-1deck-20190708103450.xls	results-cards-1deck-20190708111928.xls	740000	95%	Passed
936 3744 15912	results-cards-6deck-20190708111937.xls	results-cards-6deck-20190708113409.xls	740000	95%	Passed

Overall result: Chi-square tests passed

5. 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.

G. F. Nicoll

Geoff Nicoll
Principal Consultant
iTech Labs

20 May 2020

Kiren Sreekumar
Principal Consultant
iTech Labs

20 May 2020

Appendix – A

1. SHA-1 Signature of RNG source files

File Name	Size (bytes)	SHA-1
Slots, Card and Roulette Games		
MersenneTwisterFast.java	50643	79BECFF79A1B079F0AFB3FB5A4EF39F629F67996
Prng.java	9191	7AF62F3935270BF538EB3602F0987AB726386CC9
Slots and Card Games		
VerifyingRandom.java	1235	A149EF8932AB6745B6F1AEC03EDA37C5DB4A1648
PrngVerifyingWrapper.java	1535	385D9D332228A3B1DE6D75C368F2B57C4D6C1D03
SeedGenerator.java	3059	36B429BB5456C65462F2F1A1DB0A13857A9CF8B0
Card Games		
DeckedShoeFast.java	3943	275C81889878AF9EF18ED9A07EAF7709A3DE558B
DefaultRandom.java	1142	496E97D82A5D556A4A545491CECF185D4E02194E

2. SHA-1 Signature of executables

File Name	Size (bytes)	SHA-1
Slots, Card and Roulette Games		
MersenneTwisterFast.class	16344	581F0839DF034BD79CC2AECA3D3214B116E540C2
Prng.class	5645	15E4A3539D44C9440447A649FDBB630C59469E22
Prng$TracedNumber.class	495	2EF89196645A3E42D4EDF7CAD43CD9764B2E1EDF
Slots and Card Games		
VerifyingRandom.class	2144	784C93AB26C02D161C84C62F2DA1989866C39C01
PrngVerifyingWrapper.class	2699	7F5D34511D7A3BB27C1F93DC2374CD1E3690D83F
SeedGenerator.class	1960	A3F963F44A68D5802ECF5A919AFC2AD36730148E
Card Games		
DeckedShoeFast.class	5387	8856527F08059591230FFC97301F8C1E7984D69F
DefaultRandom.class	1870	FE3FF1D8282F79B633ABA350278537EB2F0B7A75

Appendix – B

This RNG has been certified for the following game types:

1. Slot games

2. Card games (Single deck without joker, Single deck with one joker and Six decks without joker)

3. Roulette games (European Roulette)