696/LE1541

Evaluation Report for:
GGN Europe Limited

Random Number Generator
PokerGameRNG version v1.0.0.0

Manufacturer:	**GGN Europe Limited**
RNG Name:	**PokerGameRNG v1.0.0.0**
ATF Report Number:	**RNG.DEN.GGNE.1001.01.01**
Document Number:	**01**
Date:	**17th December 2019**
Number of Pages:	**7 pages, including 2 page Annex**

BMM Spain Testlabs s.l.u

EVALUATION REPORT

Client name & Address:	GGN Europe Limited Level 3, Suite No. 2112, Tower Business Centre, Tower Street, Swatar, BKR 4013, Malta.
Client Reference Number:	Client Submission Letter Dated 15 November 2019
Testing dates:	Start date: 15 November 2019 End date: 12 December 2019
Product / Game Description:	PokerGameRNG v1.0.0.0 RNG SIGNATURES: See paragraph 4
Test Category:	Category 0
Jurisdictions Recommended:	Denmark
Technical Standard used for Evaluation:	SCP.01.03.EN.1.1. Testing Standards for Online Casino (TS)
Location where test was performed:	BMM Spain Testlabs, s.l.u. Parque Empresarial Vallsolana, Edificio Vinson Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés Barcelona – España
Location where report was issued:	BMM Spain Testlabs, s.l.u. Parque Empresarial Vallsolana, Edificio Vinson Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés Barcelona – España
Conclusion:	PASS
BMM Reference Number:	GGNE.1001
Method/Procedures used:	EURAF-SPA-MO-41 v.2.7
Consultant(s):	Enric Ferrés

1 PURPOSE OF EVALUATION

GGN Europe Limited has requested BMM to evaluate the random number generator (RNG) PokerGameRNG against the jurisdiction of Denmark.

2 DESCRIPTION OF RNG

The RNG is based on the Windows CryptoGenRandom, which is a generally recognized RNG.

3 BMM EVALUATION PERFORMED

BMM examined the RNG source code and performed statistical tests on the output from the RNG. The relevant file(s) used are listed in the section 4.

3.1 Source Code Review

The following sections describe the implementation of the RNG in the source code.

3.1.1 SEEDING

Seeded internally. The RNG is cryptographically strong and the reseeding method is not required to avoid predictability.

3.1.2 CYCLING

The RNG doesn't cycle, and the sequences are not reproducible.

3.1.3 SCALING

Scaling method does not introduce bias.

3.1.4 UNPREDICTABILITY

The RNG is cryptographically secure.

3.2 Statistical Testing

Statistical tests were performed on the output from the RNG. Raw output from the RNG was subjected to a range of tests in the Empirical, Diehard and NIST test suites. Appendix A describes the tests run in each test suite.

Each test tests the hypothesis that the RNG is a random source of numbers. A "p-value" is produced for each test run, which is the probability that a truly random process would produce the same or a more extreme result. P-values are expected to be uniformly distributed between 0 and 1. Each test is performed at least 100 times, and the p-values for each test are evaluated using an Anderson-Darling test. This produces a single p-value, which is the probability that the individual p-values have been produced from a uniform distribution.

Finally, the p-values from each test in the same test suite are combined using the Holm-Bonferroni method to provide an overall p-value. This process adjusts each p-value to ensure that the overall probability of accepting the RNG as random matches the confidence interval used. The overall p-value, equal to the minimum of the adjusted p-values, is compared to a specific alpha value to determine if the RNG is accepted or rejected as being random for a specific confidence interval.

Empirical Tests

Test	P-values	95% Confidence	99% Confidence
Frequency Test	0.703581	PASS	PASS
Serial Correlation Test	1.000000	PASS	PASS
Runs Test	0.703581	PASS	PASS
Gap Test	1.000000	PASS	PASS
Coupon Collector Test	1.000000	PASS	PASS
Subsequences Test	0.463335	PASS	PASS
Poker Test	1.000000	PASS	PASS
Overall	**0.463335**	**PASS**	**PASS**

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.
Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

Diehard Tests

Test	P-values	95% Confidence	99% Confidence
Binary Rank 32x32 Test	1.000000	PASS	PASS
Binary Rank 6x8 Test	0.626723	PASS	PASS
Birthday Spacings Test	1.000000	PASS	PASS
Bitstream Test	0.669930	PASS	PASS
Count The 1's Stream Test	1.000000	PASS	PASS
Count The 1's Specific Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Squeeze Test	1.000000	PASS	PASS
Overall	**0.626723**	**PASS**	**PASS**

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.
Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

NIST Tests

Test	P-values	95% Confidence	99% Confidence
Approximate Entropy Test	1.000000	PASS	PASS
Block Frequency Test	1.000000	PASS	PASS
Cumulative Sums Test	1.000000	PASS	PASS
Discrete Fourier Transform Test	1.000000	PASS	PASS
Frequency Test	1.000000	PASS	PASS
Linear Complexity Test	1.000000	PASS	PASS
Longest Run of Ones Test	1.000000	PASS	PASS
Non-Overlapping Template Matchings Test	1.000000	PASS	PASS
Overlapping Template Matchings Test	1.000000	PASS	PASS
Random Excursions Test	1.000000	PASS	PASS
Random Excursions Variant Test	1.000000	PASS	PASS
Rank Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Serial Test	1.000000	PASS	PASS
Universal Test	1.000000	PASS	PASS
Overall	**1.000000**	**PASS**	**PASS**

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.
Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

3.3 Additional Tests

3.3.1 MONITORING

The output of the RNG is continuously monitored and checked against the valid range for each game. When an RNG failure is detected, the internal monitoring system triggers an alarm and the game table that is affected by the RNG failure is locked.

3.3.2 MAXIMUM LOAD

BMM has generated random samples in the maximum load state on the GGNE RNG Service. Statistical tests were performed on the outputs obtained. The results of the statistical tests done indicates that the RNG performs consistently within the maximum load state.

4 SOURCE CODE FILES

The following file(s) are used by the RNG. The signatures provided are generated using SHA1.

Files	SHA1
Rhyme.Core.dll	FA5DD021A77B7411997C71711057687AEAA3989C
Deck.cs	EE41FD3E3D97CE610861A429BBA409C1C498F6CE
IDeck.cs	AEBE8589BB63A235D9A3C1897E14C0E4647C0D98

5 ADDITIONAL INFORMATION/OBSERVATIONS

N/A

6 CONCLUSION

Accordingly, from the test results[1] obtained from the testing performed and results obtained, BMM Spain Testlabs s.l.u confirms that the item submitted under test conforms to all the relevant Denmark requirements described in the Scope section.

Yours faithfully,

FRANCESCO BIANCHI
Firmado digitalmente por FRANCESCO BIANCHI
Fecha: 2019.12.17 15:19:49 +01'00'

Director of iGaming Operations EURSAM
Francesco Bianchi

MARIO ZILEVSKI
Firmado digitalmente por MARIO ZILEVSKI
Fecha: 2019.12.17 15:24:44 +01'00'

Director of Technical Services - Europe
Mario Zilevski

[1] The results included in this document are referred exclusively to the sampled tested, such as it is described in the corresponding section.

APPENDIX A STATISTICAL TESTS

The following tests were used to test the statistical properties of the RNG.

A. EMPIRICAL TESTS

The Empirical Tests are based on the tests described by Donald Knuth in The Art of Computer Programming Volume 2: Seminumerical Algorithms (1968, revised in 1997). They test sequences of numbers scaled to specific ranges.

Frequency Test	Counts of each number occurring across the sample set.
Serial Correlation Test	Counts of non-overlapping groups of numbers occurring together. Group sizes of two, three, and four are tested separately.
Runs Test	Counts of ascending and descending sequences of numbers. Note that this is a different test to the Runs Test in the Diehard and NIST Tests.
Gap Test	Counts of the size of gaps between successive occurrences of a given number. Each number in the range is tested separately.
Coupon Collector Test	Counts of sequence lengths required to complete a full set of each number in the range.
Subsequences Test	Similar to the Serial Correlation Test for pairs of numbers, except looking at numbers separated by a specific gap. Step sizes of 5, 10, 15, and 20 are tested separately.
Poker Test	The sequence is split into groups of five. The number of unique values in each group is counted.

B. DIEHARD TESTS

The Diehard Tests are based on the test suite published by George Marsaglia in 1995. They test sequences of raw binary output from the RNG.

Binary Rank 32x32 Test	Matrices are created using 32 32-bit words. The ranks of the resulting matrices are counted.
Binary Rank 6x8 Test	Same as the Binary Rank 32x32 Test, except each matrix is formed using 6 values, each taking 8 bits from successive 32-bit words with a specific offset. All possible offsets are tested separately.
Birthday Spacings Test	26-bit values are taken from successive 32-bit words with a specific offset. The values are sorted, and the spacings between them calculated. The number of spacings of the same size are counted. All possible offsets are tested separately.
Bitstream Test	Blocks of 2^18 values are treated as a stream of overlapping 20-bit values. The number of possible 20-bit values that are not found in each block is counted.
Count The 1's Stream Test	8-bit values are taken and assigned a “letter” based on the number of one’s appearing in the binary representation of each value. Overlapping groups of 5 “letters” are counted.
Count The 1's Specific Test	Similar to the Count The 1’s Stream Test, except 8-bit values are taken from successive 32-bit words with a specific offset. All possible offsets are tested separately.
Runs Test	Counts sequences of increasing and decreasing 32-bit words. Note that this is a different test to the Runs Test in the Empirical and NIST Tests.
Squeeze Test	A value of 2^31 is repeatedly multiplied by 32-bit words, dividing by 2^32 and taking the ceiling of the result each time. The number of successive words that are required to reduce the value down to 1 is counted. The value is reset to 2^31 and the process is repeated.

C. NIST TESTS

The NIST Tests are based on the suite of tests released by the National Institute of Standards and Technology in Special Publication 800-22, Revision 1a (revised April 2010). They test sequences of raw binary output from the RNG.

Approximate Entropy Test	Similar to the Serial Test, count each possible m-bit value, except it does so for two adjacent m bit lengths and compares the two.
Block Frequency Test	Similar to the Frequency Test, except the data is split into equally sized blocks. The number of ones and zeroes in each block is counted.
Cumulative Sums Test	Random walks are created by converting the data to +1 / -1 for 1 / 0 respectively and summing consecutive values.
Discrete Fourier Transform Test	The data is transformed using a Discrete Fourier Transform. The number of peaks within the 95% threshold are counted.
Frequency Test	The number of ones and zeroes in the binary output is counted.
Linear Complexity Test	The length of the linear complexity of the random sequence is determined.
Longest Run of Ones Test	The data is split into equally sized blocks. The longest run of ones in each block is determined and counted.
Non-Overlapping Template Matchings Test	The data is split into equally sized blocks. Each block is searched for a specific pattern of bits and counted. A separate test is run for various bit patterns. Each bit pattern searched does not overlap with itself. That is, when the pattern is matched, the end of the pattern cannot be the start of another match.
Overlapping Template Matchings Test	Similar to the Non-Overlapping Template Matchings Test, except only one pattern is searched, which may overlap with itself.
Random Excursions Test	As with the Cumulative Sums Test, random walks are created by converting the data to +1 / -1 for 1 / 0 respectively and summing consecutive values. The number of times a given state is visited between returns to zero are counted. Separate tests are run for various states from -4 to +4, not including 0.
Random Excursions Variant Test	Similar to the Random Excursions Test, except the number of times the given state is visited is counted for the entire sequence. Separate tests are run for various states from -9 to +9, not including 0.
Rank Test	Matrices are created using 32 32-bit words. The ranks of the resulting matrices are counted. Note that this is fundamentally the same test as the Binary Rank 32x32 Test in the Diehard Tests, although the implementation may differ.
Runs Test	Runs of consecutive bits of the same value of various lengths are counted.
Serial Test	Counts of each possible m-bit values. Separate tests are run for various m bit lengths.
Universal Test	Distances between repeated patterns of bits are counted.