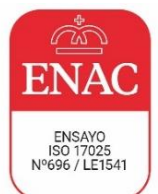


**Evaluation Report for:**  
**S.P.G. Malta Ltd**  
**Random Number Generator**  
**Random Number Generator Report version 1.0**

**Manufacturer:** Spadegaming  
**RNG Name:** Random Number Generator Report version 1.0  
**ATF Report Number:** RNG.MAL.SPG-OL.1001.01.01  
**Document Number:** 01  
**Date:** 04 April 2023  
**Number of Pages:** 8 pages, including 2 pages Annex

**BMM Spain Testlabs s.l.u.**

The content of this document is strictly confidential. It has been prepared by BMM Spain Testlabs s.l.u. (BMM) exclusively for the perusal of S.P.G. Malta Ltd and the Malta Gaming Authority and may not be disclosed to any other party without the prior written approval of S.P.G. Malta Ltd



## EVALUATION REPORT

|                                                |                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client name &amp; Address:</b>              | S.P.G. Malta Ltd<br>32, GHAR ID-DUD STREET,<br>SLIEMA SLM1572,<br>MALTA.                                                                                                                                                                                                                                                                                      |
| <b>Client Reference Number:</b>                | Client Submission Letter Dated 30 <sup>th</sup> November 2022                                                                                                                                                                                                                                                                                                 |
| <b>Testing dates:</b>                          | Start date: 19 December 2022<br>End date: 24 March 2023                                                                                                                                                                                                                                                                                                       |
| <b>Product / Game Description:</b>             | Random Number Generator Report<br>version 1.0<br>RNG Software<br>SIGNATURES: See paragraph 5                                                                                                                                                                                                                                                                  |
| <b>Test Category:</b>                          | RNG Evaluation                                                                                                                                                                                                                                                                                                                                                |
| <b>Jurisdictions Recommended:</b>              | Malta                                                                                                                                                                                                                                                                                                                                                         |
| <b>Technical Standard used for Evaluation:</b> | <ul style="list-style-type: none"> <li>Remote Gambling Regulations officially published on the 20th April 2004 (currently in force as long as technical standards of the 2018 Gaming Act are not published)</li> <li>Player Protection Directive (in force 1.8.2018 apart from some articles coming into force on 31.3.2019) (amended 28 May 2021)</li> </ul> |
| <b>Location where test was performed:</b>      | BMM Spain Testlabs, s.l.u.<br>Parque Empresarial Vallsolana, Edificio Vinson<br>Camí de Can Camps, 17-19<br>08174 Sant Cugat del Vallés<br>Barcelona – España                                                                                                                                                                                                 |
| <b>Location where report was issued:</b>       | BMM Spain Testlabs, s.l.u.                                                                                                                                                                                                                                                                                                                                    |
| <b>Conclusion:</b>                             | PASS                                                                                                                                                                                                                                                                                                                                                          |
| <b>BMM Reference Number:</b>                   | SPG-OL.1001                                                                                                                                                                                                                                                                                                                                                   |
| <b>Method/Procedures used:</b>                 | EURSAM-SPA-MO-41 v.2.9                                                                                                                                                                                                                                                                                                                                        |
| <b>Consultant(s):</b>                          | Slava Kolmykov                                                                                                                                                                                                                                                                                                                                                |

## 1. SCOPE OF EVALUATION.

S.P.G. Malta Ltd has requested BMM to evaluate the random number generator (RNG) Random Number Generator Report v 1.0 against Malta:

- Remote Gambling Regulations officially published on the 20<sup>th</sup> April 2004 (currently in force as long as technical standards of the 2018 Gaming Act are not published)
- Player Protection Directive (in force 1.8.2018 apart from some articles coming into force on 31.3.2019) (amended 28 May 2021)

## 2. DESCRIPTION OF RNG.

The RNG is an implementation of java.security.SecureRandom library.

## 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 5.

### 3.1. Source Code Review.

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

#### 3.1.1 SEEDING.

No Additional seeding is required.

#### 3.1.2 CYCLING.

The RNG does not cycle.

#### 3.1.3 SCALING.

The scaling method does not introduce bias.

#### 3.1.4 UNPREDICTABILITY.

The RNG is crypto-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. 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          | 0,573741        | PASS           | PASS           |
| Serial Correlation Test | 1,000000        | PASS           | PASS           |
| Runs Test               | 1,000000        | PASS           | PASS           |
| Gap Test                | 1,000000        | PASS           | PASS           |
| Coupon Collector Test   | 1,000000        | PASS           | PASS           |
| Subsequences Test       | 1,000000        | PASS           | PASS           |
| Poker Test              | 0,573741        | PASS           | PASS           |
| <b>Overall</b>          | <b>0,573741</b> | <b>PASS</b>    | <b>PASS</b>    |

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        | 1,000000        | PASS           | PASS           |
| Birthday Spacings Test      | 1,000000        | PASS           | PASS           |
| Bitstream Test              | 1,000000        | 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           |
| <b>Overall</b>              | <b>1,000000</b> | <b>PASS</b>    | <b>PASS</b>    |

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                               | 0,207876        | PASS           | PASS           |
| Serial Test                             | 1,000000        | PASS           | PASS           |
| Universal Test                          | 1,000000        | PASS           | PASS           |
| <b>Overall</b>                          | <b>0,207876</b> | <b>PASS</b>    | <b>PASS</b>    |

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

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

#### 4. EVALUATION OF THE TECHNICAL REQUIREMENTS.

BMM has tested and confirmed compliance of the RNG against the appropriate applicable technical requirements for Malta. BMM performed the following tests to confirm compliance to the relevant regulatory specifications:

| DESCRIPTION                                                                                                                                                                                                                                 | PASS           | FAIL                     | N/A                      | NOTES |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------|--------------------------|-------|
|                                                                                                                                                                                                                                             | EXTERNAL REF # |                          |                          |       |
| The gaming system must satisfy the following criteria for randomness, following Schneier:                                                                                                                                                   | X              | <input type="checkbox"/> | <input type="checkbox"/> |       |
|                                                                                                                                                                                                                                             | 3              |                          |                          |       |
| (a) the data must be randomly generated, passing appropriate statistical tests of randomness                                                                                                                                                | X              | <input type="checkbox"/> | <input type="checkbox"/> |       |
|                                                                                                                                                                                                                                             | 3 a)           |                          |                          |       |
| (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 | X              | <input type="checkbox"/> | <input type="checkbox"/> |       |
|                                                                                                                                                                                                                                             | 3 b)           |                          |                          |       |
| (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.                       | X              | <input type="checkbox"/> | <input type="checkbox"/> |       |
|                                                                                                                                                                                                                                             | 3 c)           |                          |                          |       |

#### 5. SOURCE CODE FILES.

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

| Files               | SHA1                                     |
|---------------------|------------------------------------------|
| Random-20230130.jar | 473072BB96768D50144CB2C23E66CAF2CFB9E541 |

#### 6. ADDITIONAL INFORMATION/OBSERVATIONS.

N/A

## 7. CONCLUSION.

According to the test results<sup>1</sup>, BMM Spain Testlabs s.l.u. confirms that the item submitted for testing is compliant with all the relevant Regulations listed in Scope of Evaluation section.

Yours faithfully,

Rubén Baptista  
**Senior Director of Service Delivery Europe and South America**

<sup>1</sup>The results included in this document are referred exclusively to the sampled tested, such as it is described in the corresponding section.

This test report may not be reproduced, other than in full, except with the prior written permission of the issuing BMM Spain Testlabs, s.l.u.

## Appendix A STATISTICAL TESTS

### 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.                                                                           |

### 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      | 32-bit words are taken as values, sorted, and the spacings between them calculated. The number of spacings of the same size are counted.                                                                                                                                                  |
| 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. |

## 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.                                                                                                                                                                                                                                                                    |