BMM EVALUATION TEST REPORT

Report Issue Date:	11th June 2026
Issued To:	RTG Slots Gaming
Issued By:	BMM Testlabs Travis Foley, Executive Vice President, Operations 815 Pilot Road, Suite G, Las Vegas, NV 89119 (702) 407 2420, www.bmm.com A2LA # 2549.01
Evaluation By:	BMM Testlabs, 815 Pilot Road, Suite G, Las Vegas, NV 89119
Manufacturer:	World Genesis Limited 14/F China Hong Kong Tower, 8 Hennessy Road, Wanchai, Hong Kong
Evaluation for:	CSRNG 1.0.0.0
Reference Numbers:	
BMM:	ITS.1001
Report Number:	ITS10011-WGL-RNG_E

1. STANDARD TESTED TO / RESULT

Technical Standard Used for Compliance Evaluation	Test Result	
	Pass	Fail
GLI-19, Standards for Interactive Gaming Systems, version 3.0, dated July 17, 2020	☑	☐

2. PURPOSE

World Genesis Limited has requested BMM to perform an evaluation of the CSRNG 1.0.0.0. The evaluation was conducted against the aforementioned industry recognized standards for Random Number Generator (RNG) testing.

This evaluation includes an assessment of the algorithm implemented within the RNG 1.0.0.0.

3. SCOPE OF WORK

The evaluation of the CSRNG 1.0.0.0 consisted of a source code review and statistical tests.

The purpose of the source code review is to document and verify the following:

- Identify the RNG algorithm and verify its implementation.
- The RNG is used correctly based on the design and parameters of the system.
- Verify the seeding method is based on an uncontrolled event.
- Determine the period of the RNG and confirm if it is sufficiently large enough for the game design.
- The RNG algorithm is capable of generating numbers or values that are scaled accurately for the system design.
- The method of generating scaled numbers or values is unbiased and unpredictable.
- The RNG source code does not contain any malicious code that could significantly affect the outcome of the RNG.

The industry recognized standard for statistical testing includes, but is not limited to: Frequency, Serial Correlation, Run, Gap, Coupon Collector, Subsequences, and Poker Tests, Diehard suite and NIST suite of tests. These tests are intended to verify the statistical properties of the RNG output and demonstrate the correct use of the RNG. Refer to Appendices 1, 2, and 3 for a detailed explanation of the statistical tests performed.

4. EVALUATION RESULTS

The source code review of the RNG and empirical statistical RNG testing of the CSRNG 1.0.0.0 confirms:

- The RNG algorithm is HMAC-DRBG using SHA-256, and its implementation has been verified.
- The proper usage of the RNG has been verified throughout the system.
- The seeding method of the RNG is based on cryptographically sourced entropy from the operating system.

- The period size of the RNG is 2^{32}, and it is sufficiently large enough for the game design.
- The RNG algorithm is capable of generating numbers or values that are scaled accurately for the system design.
- The method of generating scaled numbers or values is unbiased and unpredictable.
- The RNG source code does not contain any malicious code that could significantly affect the outcome of the RNG.
- The overall results of the statistical tests are probabilities that, using the Holm method, meet the 95% and 99% jurisdictional required confidence interval. Refer to Appendices 1, 2, and 3 which contain the resulting p-values for the Empirical tests, Diehard test suite, and the NIST test suite, respectively.

Each statistical test results in a probability value, which is also called a p-value, which is the probability that a true random source would produce the same or a more extreme result. When multiple tests are run for an RNG sample, the probability of at least one (1) test failing at a given confidence interval becomes much larger than the intended alpha level, even if the RNG sample came from a truly random source. This issue is called the Family-Wise Error Rate in mathematical terms. To counteract this issue, the p-values from each test are adjusted so that the overall probability of accepting the RNG sample as random matches the confidence interval. BMM uses the Holm - Bonferroni Method which is:

- Each p-value is ranked from one (1) to n, for n sub-tests in order of ascending value.
- Each p-value is multiplied by (n – *i* + 1), where *i* is the rank.
- The adjusted p-value is capped to a maximum value of one (1).
- The adjusted p-value for item *i* is then set to the maximum of all adjusted p-values for items one (1) to *i*.

The smallest p-value is then compared to an alpha level to determine if the sequence is accepted or rejected as random. The alpha level is determined by the confidence interval. For example, a confidence interval of 95% compares p-values to an alpha level of 5%, or 0.05. Since the p-values are expected to be uniformly distributed, it is expected that a true random source would produce rejected sequences 5% of the time for a 95% confidence interval. Therefore, the value of each individual p-value is not considered by itself to determine success or failure.

5. EVALUATION DETAILS

5.1. Software Version Details:

The following table details the relevant information for the CSRNG 1.0.0.0 that has been evaluated as compliant to aforementioned RNG Technical Standard:

Product ID	Product Version	Product Type	File / Folder	Signature	Signature Type
CSRNG	1.0.0.0	RNG	RNG.cpp	23E8CB473FF43A5119FB488A5 D4EE28B9F8133B8	SHA-1
CSRNG	1.0.0.0	RNG	HashBasedDRBG.h	CB8A46D5135462B4E25C9EB88 44B459C60AFA55E	SHA-1

Product ID	Product Version	Product Type	File / Folder	Signature	Signature Type
CSRNG	1.0.0.0	RNG	CSRNG.h	118739266920D8C611139848D ED77DE84345FAE6	SHA-1
CSRNG	1.0.0.0	RNG	SeedConstants.h	2122B2A252E654F945346B516 199D46F81F1BA7E	SHA-1
CSRNG	1.0.0.0	RNG	CSRNGExport.h	89CB2714D3A3FE8C595EF633B F3FC2B9510AC53E	SHA-1
CSRNG	1.0.0.0	RNG	ObjectPool.h	8DA61879038C9BAF7A261380C BB932B2C7F9E279	SHA-1
CSRNG	1.0.0.0	RNG	fileversion.h	9A7A42D1BDC12544CAB6A290 F3BDA1A0E69639E1	SHA-1
CSRNG	1.0.0.0	RNG	CSRNG.dll	9B7225532938015E31FF3F02E6 FE4C5A0797972E	SHA-1
CSRNG	1.0.0.0	RNG	\cryptopp610	4FE1FDCC834F1B55F5E6F2B1EB 79501E67C4B3CE	SHA-1
Location: Server Validation Program Used: BMM Signatures v2.0.6					

***Note**: Refer to Section 6.1 for verification tools used.*

6. DEVICE IDENTIFICATION

6.1. Software Signature Verification Information:

Signature Verification Application:

1. The SHA-1 signatures were calculated and verified using the BMM Signatures proprietary verification tool, which has been calibrated in accordance with ISO/IEC 17025 sections 6.4.1, 6.4.8, 6.4.13 (a), and 6.4.13 (c); as well as ISO/IEC 17020 sections 6.2.4, 6.2.6, 6.2.13 (a), and 6.2.15.
2. Where requested, BMM will supply the regulator/operator with BMM's proprietary verification tool "BMM Signatures" for verifying the SHA-1 details above. A user manual will also be supplied.
3. Signature verification procedures may require administrator rights access.

Signature Verification Procedure:

1. Install BMM Signatures v2.0.6 on the computer to be used for software verification and double click on the "BMM Signatures" icon.
2. The BMM Signatures program will open.
3. Ensure that the correct BMM Signatures version is selected in the Version drop down menu.

Signature Verification for Individual Files

1. Select the "Files/Folders" tab.
2. Select the “Browse Files” button in BMM Signatures.
3. Navigate to the appropriate directory and select the files shown in Section 5.1 of this report.
4. Select the “Open” button from the window.
5. Repeat the steps listed above for each file to be verified, they will appear listed in the “File Location” and “Name” columns.
6. Click the desired algorithm to use (e.g. SHA1). When the program is completed, the signatures will be displayed in the Output window.
7. Verify that the software file signatures obtained match those listed in Section 5.1 of this report.

7. ADDITIONAL NOTES

- Appendix 1 contains the results and definitions for the Empirical tests.
- Appendix 2 contains the results and definitions for the Diehard test suite.
- Appendix 3 contains the results and definitions for the NIST test suite.

8. CONCLUSION

An evaluation of the CSRNG 1.0.0.0 was performed to verify CSRNG 1.0.0.0 meets the aforementioned industry recognized standards for Random Number Generator (RNG) testing.

In accordance with the scope for this project, BMM Testlabs finds that the CSRNG 1.0.0.0 outcomes demonstrate the RNG is implemented correctly and demonstrates statistical randomness. The Empirical tests, Diehard tests, and NIST tests all pass a 95% and 99% confidence interval.

9. TERMS AND CONDITIONS

BMM Testlabs ("BMM") has conducted a level of testing of the gaming product which has historically been adequate for a submission of this type. However, inherent in testing in a laboratory environment are the unavoidable limitations of not being able to verify the effects of all possible configurations and environments that occur in actual gaming venues.

This evaluation report is for use by the client for the jurisdiction ("Jurisdiction") referenced in the report (the "Report") and only verifies, as of the date stated, the gaming product described in the Report subject to any conditions or limitations set forth therein.

The manufacturer named in the Report is solely responsible for possession of the appropriate license to sell, lease, service, or provide gaming supplies or gaming-related services in the Jurisdiction and for compliance with the ongoing requirements of the Jurisdiction. It is the responsibility of the manufacturer and operators to ensure that the gaming product detailed in this Report is installed, maintained and operated correctly without defects and safely in accordance with requirements of the Jurisdiction.

The Report and testing performed by BMM is proprietary to BMM. This Report is issued solely for the benefit of the client and shall not be reproduced, reprinted, or transmitted in whole or in part to any party not named in the Report without the written approval of BMM, other than by a regulator of the Jurisdiction. No third party may use, rely, or refer to the Report, its contents, or any related documents, without written permission of BMM. If BMM grants consent, BMM will send this Report via email as directed. BMM takes precautionary measures to secure the "PDF" document, but BMM does not send the email via any encrypted methodology.

The undersigned certifies under penalty of perjury that the compliance testing of the gaming product detailed in this Report and any accompanying documents was conducted in accordance with the requirements of the Jurisdiction and that the gaming product meets the requirements of its laws and the regulations adopted thereunder, and all published technical standards, control standards, control procedures, policies, industry notices and similar requirements implemented or issued by the Jurisdiction to the best of BMM's knowledge and belief.

Notwithstanding the above, any regulator may reprint, reproduce and transmit any document or information to any party that the regulator, in their sole discretion, deems appropriate.

BMM DOES NOT MAKE, AND EXPRESSLY DISCLAIMS, ALL OTHER WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, SUITABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE LIABILITY AND OBLIGATIONS OF BMM HEREUNDER, AND THE REMEDY OF THE RECIPIENT, UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO, AT BMM'S OPTION, REPLACEMENT OF THE SERVICES PROVIDED OR THE REFUND BY BMM OF ANY MONIES RECEIVED BY IT FOR THE SERVICES PROVIDED. IN NO EVENT SHALL BMM BE RESPONSIBLE TO THE CLIENT OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS OR REVENUE, BUSINESS INTERRUPTION, OR PUNITIVE DAMAGES, EVEN IF BMM HAD BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES.

Please feel free to contact BMM Testlabs if you have any questions in regards to this evaluation report.

Yours sincerely,

Travis Foley
Executive Vice President, Operations
BMM Testlabs

T/ lm
G/ jm

v7.9

Appendix 1:

Empirical Test Results

The results of the Emprical tests are probabilities (p-values) that are evaluated using the Holm Method to verify the confidence interval. The Empirical Tests are based on the tests described by Donald Knuth in The Art of Computer Programming Volume 2: Seminumerical Algorithms (1997). They test sequences of numbers scaled to specific ranges.

Test	Description
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.

Empirical Tests

Test	P-values	95% Confidence	99% Confidence
Frequency Test	1.000000	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	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.

Appendix 2:

Diehard Test Results

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.

Test	Description
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 232 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, and the value is reset to 231 and the process repeated.

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

Test	P-values	95% Confidence	99% Confidence
Count The 1's Specific Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Squeeze 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.

Appendix 3:

NIST Test Results

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.

Test	Description
Approximate Entropy Test	Similar to the Serial Test, count each possible m-bit values, 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 equal size 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 equal size blocks. The longest run of ones in each block is determined and counted.
Non-Overlapping Template Matchings Test	The data is split into equal size 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 Templates Test, except only one pattern is searched, which may overlap with itself.
Random Excursions Test	As with the Cumulative Sum 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.

Test	Description
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.

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.