Evaluation Report for
Redstar Lotus Nigeria Limited
Lottery Random Number Generator
Version 1.0.0

ATF Report Number:	**NGA.REDSTAR.1001.01**
Date:	**6 December 2024**
Document Number:	**1**
Number of Pages:	**14**

BMM Testlabs South Africa (Pty) Ltd

bmmtestlabs southafrica (pty) ltd is a SANAS accredited testing laboratory number T0290 to ISO17025

Disclaimer: All results in this test report are subcontracted results.

Evaluation Report

Manufacturer Name & Address:	Redstar Lotus Nigeria Limited 56 Toyin Street, Ikeja Lagos, Nigeria
Manufacturer Reference Number:	Client Submission Letter Dated 22nd October 2024
Testing dates:	Start date: 15th November 2024 End date: 21st November 2024
Product /Game Description:	Random Number Generator
Jurisdictions Recommended:	Nigeria
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 Testlabs South Africa (Pty) Ltd No. 10 Brands Hatch Close, Kyalami Business Park Kyalami, Midrand 1685 South Africa
Conclusion:	Pass
BMM Ref Number:	REDSTAR.1001
Consultant(s):	Gianni Piccioni

TECHNICAL STANDARD(S) TESTED AGAINST

Technical Standard(s) used for Compliance Evaluation:	Comply		
	Yes	No	N/A
GLI Standard Series, GLI-19: Standards for Interactive Gaming Systems, Version: 3.0, Revision Date: July 17, 2020.	☒	☐	☐

Approval Conditions
None

1. PURPOSE

Redstar Lotus Nigeria Limited., requested BMM Testlabs South Africa (Pty) Ltd., hereinafter referred to as BMM, to evaluate Lottery Random Number Generator Version 1.0.0 for satisfactory operation in the relevant Nigerian Gambling market.

***Disclaimer**: All Random Number Generator evaluation below is a subcontracted test by an ENAC accredited testing laboratory, BMM Spain, Inc., accreditation number 696/LE1541.*

2. PRODUCT CHARACTERISTICS (PRODUCT UNDER TEST)

The Random Number Generator uses the module "System.Securiry.cryptography.RandomNumberGeneator" from C# to generate cryptographically secure numbers.

3. BMM EVALUATION PERFORMED (SAMPLE UNDER TEST)

BMM has tested and confirmed compliance of the Lottery Random Number Generator Version 1.0.0 against the appropriate applicable technical requirements for the relevant Nigerian Gambling markets. BMM performed the following tests to confirm compliance to the relevant regulatory specifications:

3.1 Random Number Generator Evaluation

This test was performed to evaluate and verify that the random number generation is as specified in the technical documentation supplied by the manufacturer meets the requirements specified in technical standard. BMM has verified, through mathematical and statistical analysis, that the Random Number Generator (RNG) distributes numbers with fair distribution, lack of bias to particular outcomes and sufficient non-predictability.

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

3.2.1 Seeding

Lottery Random Number Generator Version 1.0.0

3.2.2 Cycling

The RNG does not cycle because it's cryptographically secure.

3.2.3 Scaling

The scaling function performs a modulo operation and does not introduce bias.

3.2.4 Unpredictability.

The RNG is cryptographically secure and uses sources of entropy to change its state, therefore it is unpredictable.

3.2.5 Software Details:

Product ID	Product Function	File Name	SHA1
GDLottoSecureRandomLibrary.dll	Random Number Generator	GDLottoSecureRandomLibrary.dll	AEB2F8FDAC407170DD2AAE5793A8CD07706C81D6

3.2.6 Statistical Test Results

Statistical tests were performed on the output from the RNG. Raw output from the RNG was subjected to a range of tests in the Diehard and NIST test suites.
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	0,846832	PASS	PASS
Serial Correlation Test	1,000000	PASS	PASS
Runs Test	0,846832	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	0,846832	**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	1,000000	PASS	PASS
Birthday Spacings Test	0,206519	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
Overall	0,206519	**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	0,371583	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	0,371583	**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.

4. EVALUATION OF THE TECHNICAL REQUIREMENTS.

BMM has tested and confirmed compliance of the RNG against the appropriate applicable technical requirements for GLI-19 v3.0 standard. BMM performed the following tests to confirm compliance to the relevant standard specifications:

Description	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
COMPLIANCE TESTING				
Source Code Review				
The independent test laboratory shall review the source code pertaining to any and all core randomness algorithms, scaling algorithms, shuffling algorithms, and other algorithms or functions that play a critical role in the final random outcome selected for use by a game.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.1			
This review shall include comparison to published references, where applicable, and an examination for sources of bias, errors implementation, malicious code, code with the potential to corrupt behavior, or undisclosed switches or parameters having a possible influence on randomness and fair play.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.1			
Game Selection Process				
After selection of the game outcome, the game shall not display a “near miss” where it makes a variable secondary decision which affects the result shown to the player.	☐	☐	☒	Just RNG Evaluation.
	GLI 19 v3.0 § 4.5.2 (c)			

Description	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
COMPLIANCE TESTING				
Statistical Analysis -Applied Tests				
The independent test laboratory shall employ statistical tests to assess the outcomes produced by the RNG, after scaling, shuffling, or other mapping (hereafter referred to as "final outcome output").	☒	☐	☐	
	GLI 19 v3.0 § 3.2.2			
The independent test laboratory shall choose appropriate tests on a case-by-case basis, depending on the RNG under review and its usage within the game.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.2			
The tests shall be selected to assure conformance to intended distribution of values, statistical independence between draws, and, if applicable, statistical independence between multiple values within a single draw.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.2			
The applied tests shall be evaluated, collectively, at a 99% confidence level.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.2			
The amount of data tested shall be such that significant deviations from applicable RNG testing criteria can be detected with high frequency. In the case of an RNG intended for variable usage, it is the responsibility of the independent test laboratory to select and test a representative set of usages as test cases.	☒	☐	☐	5 samples of 1M numbers and 1 sample of 10M numbers
	GLI 19 v3.0 § 3.2.2			
These tests may include, but are not limited to:	GLI 19 v3.0, § 3.2.2			
Total Distribution Test or Chi-Square test;	☒	☐	☐	
	GLI 19 v3.0, § 3.2.2 (a)			
Overlaps test;	☒	☐	☐	
	GLI 19 v3.0, § 3.2.2 (b)			
Coupon collector's test;	☒	☐	☐	
	GLI 19 v3.0, § 3.2.2 (c)			
Runs tests (patterns of occurrences should not be recurrent);	☒	☐	☐	
	GLI 19 v3.0, § 3.2.2 (d)			
Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);	☒	☐	☐	*GLI-19 v3.0 § 3.2.2 f) Serial Correlation test*
	GLI 19 v3.0, § 3.2.2 (f)			

Description	Pass	Fail	N/A	Notes
	External Ref #			
Compliance Testing				
Duplicates test.	☒	☐	☐	
	GLI 19 v3.0, § 3.2.2 (g)			
Available Outcomes				
As verified by source code review, the set of possible outcomes produced by the RNG solution (i.e., the RNG period), taken as a whole, shall be sufficiently large to ensure that all outcomes shall be available on every draw with the appropriate likelihood, independent of previously produced outcomes, except where specified by the game design.	☒	☐	☐	This is a cryptographic RNG that uses entropy, so there is no cycle.
	GLI 19 v3.0 § 3.2.5			
Distribution				
Each possible RNG selection shall be equally likely to be chosen.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.3			
Where the game design specifies a non-uniform distribution, the final outcome shall conform to the intended distribution.	☐	☐	☒	Just RNG Evaluation
	GLI 19 v3.0 § 3.2.3			
All scaling, mapping, and shuffling algorithms used shall be unbiased, as verified by source code review. The discard of RNG values is permissible in this context and may be necessary to eliminate bias	☒	☐	☐	
	GLI 19 v3.0 § 3.2.3 (a)			
The final outcome output shall be tested against intended distribution using appropriate statistical tests (e.g., Total Distribution test).	☒	☐	☐	
	GLI 19 v3.0 § 3.2.3 (b)			
Independence				
Knowledge of the numbers chosen in one draw shall not provide information on the numbers that may be chosen in a future draw. If the RNG selects multiple values within the context of a single draw, knowing one or more values shall not provide information on the other values within the draw, unless provided for by the game design.	☒	☐	☐	
	GLI 19 v3.0 § 3.2.4			
As verified by source code review, the RNG shall not discard or modify selections based on previous selections, except where intended by game design (e.g., without-replacement functionality); and	☐	☐	☒	Just RNG Evaluation.
	GLI 19 v3.0 § 3.2.4 (a)			

Description	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
COMPLIANCE TESTING				
The final outcome output shall be tested for independence between draws and, as applicable, independence within a draw, using appropriate statistical tests (e.g., Serial or Interplay Correlation tests, and Runs test).	☒	☐	☐	
	GLI 19 v3.0 § 3.2.4 (b)			
Card Games				
At the start of each game and/or hand, the cards shall be drawn from a randomly shuffled deck(s). It is acceptable to draw random numbers for replacement cards at the time of the first hand's random number draw, provided that the replacement cards are sequentially used as needed, and so long as any stored RNG values are encrypted	☐	☐	☒	Not a Card Game, Just RNG Evaluation.
	GLI 19 v3.0 § 4.4.4 (a)			
As cards are removed from the deck they shall be immediately used as directed by the rules of the game (i.e., the cards are not to be discarded due to adaptive behavior by the gaming device)	☐	☐	☒	Not a Card Game, Just RNG Evaluation.
	GLI 19 v3.0 § 4.4.4 (b)			
The deck(s) shall not be reshuffled except as provided by the rules of the game.	☐	☐	☒	Not a Card Game, Just RNG Evaluation.
	GLI 19 v3.0 § 4.4.4 (c)			
	GLI 19 v3.0 § 4.5.1 (b)			
Hardware-Based RNG Games				
<u>Dynamic Output Monitoring.</u> Due to their physical nature, the performance of hardware-based RNGs may deteriorate over time or otherwise malfunction, independent of the gaming device [platform]. The failure of a hardware-based RNG could have serious consequences for the intended usage of the RNG. For this reason, if a hardware-based RNG is used, there shall be dynamic monitoring of the output by statistical testing. This monitoring process shall disable game play when malfunction or degradation is detected.	☐	☐	☒	Software RNG
	GLI 19 v3.0 § 3.3.3			
Mechanical Based RNG Games/Physical Randomness Device				
<u>Data Collection Amount.</u> To provide best assurance of random behavior, the independent test laboratory shall collect game outcome data for at least 10,000 game outcomes.	☐	☐	☒	Software RNG.
	GLI 19 v3.0 § 3.4.2			

Description	Pass	Fail	N/A	Notes
	External Ref #			
Compliance Testing				
Data Collection Procedures. The data collection shall be accomplished in a fashion reasonably similar to the intended use of the device in the field. In particular, the recommended setup and calibration shall be executed initially, and the device and components (cards, balls, etc.) shall be replaced or serviced during the collection period as recommended by the manufacturer.	☐	☐	☒	Software RNG.
	GLI 19 V3.0 § 3.4.2			
All mechanical pieces shall be constructed of materials to prevent degradation of any component over its intended lifespan.	☐	☐	☒	Software RNG.
	GLI 19 v3.0 § 3.4.3			
Tampering. The player / game operator (gaming attendants-e.g., dealers, croupiers, etc.) shall not have the ability to manipulate or influence the mechanical RNG [physical randomness devices] in a physical manner with respect to the production of game outcomes, except as intended by game design.	☐	☐	☒	Software RNG.
	GLI 19 v3.0 § 3.4.4			
Cryptographic RNG				
The RNG used in the determination of game outcomes in a Gaming Platform **shall** be cryptographically strong. "Cryptographically strong" means that the RNG is resistant to attack or compromise by an intelligent attacker with modern computational resources, and who may have knowledge of the source code of the RNG.	☒	☐	☐	
	GLI 19 v3.0 § 3.3.1			
A cryptographic RNG cannot be feasibly compromised by a skilled attacker with knowledge of the source code. At a minimum, cryptographic RNGs shall be resistant to the following types of attack:	☒	☐	☐	
	GLI 19 v3.0 § 3.3.2			
Direct Cryptanalytic Attack: Given a sequence of past values produced by the RNG, it shall be computationally infeasible to predict or estimate future RNG values. This must be ensured through the appropriate use of a recognized cryptographic algorithm (RNG algorithm, hash, cypher, etc.);	☒	☐	☐	
	GLI 19 v3.0 § 3.3.2 (a)			

Description	Pass	Fail	N/A	Notes
	External Ref #			
Compliance Testing				
Known Input Attack: It shall be infeasible to computationally determine or reasonably estimate the state of the RNG after initial seeding. In particular, the RNG must not be seeded from a time value alone. The manufacturer must ensure that games will not have the same initial seed, even when powered -on or booted simultaneously. Seeding methods shall not compromise the cryptographic strength of the RNG; and	☒	☐	☐	RNG is cryptographically secure.
	GLI 19 v3.0 § 3.3.2 (b)			
State Compromise Extension Attack: The RNG shall periodically modify its state, through the use of external entropy, limiting the effective duration of any potential exploit by a successful attacker.	☒	☐	☐	RNG is cryptographically secure.
	GLI 19 v3.0 § 3.3.2 (c)			
Physiscs Engine				
Games may utilize a "physics engine" which is specialized software that approximates or simulates a physical environment, including behaviors such as motion, gravity, speed, acceleration, inertia, trajectory, etc. A physics engine shall be designed to maintain consistent play behaviors and game play environment unless an indication is otherwise provided to the player by the game artwork. A physics engine may utilize the random properties of an RNG to impact game outcome, in which case, the RNG requirements shall apply.	☐	☐	☒	Software RNG.
	GLI 19 v3.0 § 4.6.3			

5. ADDITIONAL INFORMATION.

N/A

6. SOFTWARE SIGNATURE VERIFICATION

6.1 **Signature Verification Procedure:**

- Open the "BMM Signatures 2.0.6" application tool.
- Select option "browse files".
- Locate the file from the where it is saved.
- Add all files by clicking the "open" button on the open dialog window.
- Select the digital signature (SHA1) to be calculated.
- The "BMM Signatures 2.0.6" application tool will calculate the signatures and the signatures will be displayed in the output panel.
- Save the results to a desired directory using the "export" button.

- The results will be saved as a csv file.
- The signatures can be compared to the signatures listed in this report

NB: *Where requested, BMM will supply the regulator/operator with BMM's proprietary verification tool* "BMM Signatures 2.0.6". A user manual will also be supplied.

7. CONCLUSION

As a result of statistical testing and source code review, BMM confirms that the Lottery Random Number Generator Version 1.0.0 provides uniformly random data suitable for its intended application. This RNG complies with the applicable requirements for operation in Nigeria

8. COMPLIANCE CONFORMITY

BMM Testlabs South Africa (Pty) Ltd., has conducted a level of testing which has historically been adequate for a submission of this type. However, inherent in testing in a laboratory environment is the unavoidable limitations of it not being possible to verify the effects of all possible configurations and environments that occur in actual gaming venues. Accordingly, subject to the above comment, from the testing performed BMM Testlabs South Africa (Pty) Ltd. Confirms that the item under test (unless otherwise stated) conforms to the relevant Nigerian technical requirements.

The results relate only to the items tested.

This report shall not be reproduced except in full without approval of the laboratory.

Disclaimer 1*: BMM allows its clients to review the draft BMM Evaluation Report for content before it is sent to the NRCS. If BMM receives no queries within 30 days from date of issue as stated on page 1 of the BMM Evaluation Report, BMM Testlabs South Africa (Pty) Ltd., will take the report as correct and accepted.*

Disclaimer 2*: BMM shall not be liable to any other party with respect to the undertaking of this project, BMM will not and cannot warrant or guarantee, expressly or impliedly, any aspect of the product. BMM is not responsible for either the action or inaction of any governmental or regulatory authority.*

Yours sincerely,

Digitally signed by Ntakuseni Andrew Matamela
Date: 2024.12.06 08:54:04 +02'00'

Ntakuseni Matamela

Team Leader

APPENDIX A

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

A1. 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.

A2. 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.

A3. 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.

-End of Document-