

Certification Report: Global Game Internusa B.V RNG Evaluation

Report Identification: LTI-CW-230808-01-RC-R1

Certification Laboratory:



Supervisor: Usman Vasser

Signatures:

A handwritten signature in black ink, appearing to read 'Usman Vasser'.

Certifier: Wajahat Kashan

ISO/IEC 17025: UKAS accredited testing laboratory No. 9263

Dates of certification work: 17 July 2023 to 31 July 2023

Date of issue of certification report: 08 August 2023

Report prepared for: Global Game Internusa B.V (Global Games)
Julianaplein 36,
Curacao

Jurisdiction: Curaçao eGaming

Technical Standard used for testing: GLI-19: Standards for Interactive Gaming System
Version: 3.0

Gaming Associates

1 Notations

1.1 Confidentiality

This document, all related documents, and methodologies embodied in this document and related documents (“the documents”) are the property of Gaming Associates Europe Limited (hereinafter referred to as Gaming Associates or **ga**). Unauthorised copying and distribution of the documents, by any means, on any media are prohibited.

This document, its themes, and ideas are strictly confidential and may not be used in any manner other than its expressed purpose, without the written permission of the author. The documents are for the intended client named in this report, also referred to as “the client” or “client”, and the applicable gaming jurisdiction mentioned in this document.

The documents are copyright.

1.2 Disclaimer

ga has reported on what was discovered throughout the assessment of the client’s RNG as per applicable jurisdictional requirements. Results are based on the client’s submission of information material, interview with the technical staff, and verification of the information security controls.

ga has undertaken its best endeavours to ensure a thorough assessment is performed and the conclusion stated.

2 Administration

2.1 Contents

1	Notations	2
1.1	Confidentiality	2
1.2	Disclaimer.....	2
2	Administration	3
2.1	Contents.....	3
2.2	Version.....	3
3	Executive summary	4
3.1	Introduction	4
3.2	RNG details.....	4
3.3	Scope of evaluation.....	4
3.4	Conclusions and Recommendations	4
4	Test Results	5
4.1	Chapter 3: Random Number Generator (RNG) Requirements	5
5	References	10
	Annex A : Statistical testing of raw pRNG output.....	11
A.1	Diehard test results.....	11
A.2	Scaled data statistical testing results.....	13
	Annex C: Hashes of RNG	14
	End of document.....	15

2.2 Version

Version	Description	Date
V0.1	Initial draft – KALI	2023-08-01
V0.2	Review & Updated – WKAS	2023-08-02
V0.3	QA – UVAS	2023-08-03
V1.0	Final Report to Global Games	2023-08-08

3 Executive summary

3.1 Introduction

Global Game Internusa B.V (Global Games) has requested Gaming Associates (**ga**) to evaluate their pseudo-Random Number Generator (pRNG) being used in online games for Curaçao eGaming against GLI-19: Standards for Interactive Gaming System Version: 3.0.

This report presents the results of evaluation performed by **ga** for the RNG for Curaçao eGaming against Chapter 3: Random Number Generator (RNG) Requirements of GLI-19: Standards. Hashes of source code and binary files related to the RNG are listed in Annex C of this report.

3.2 RNG details

Global Games is using PHP with the implementation of Mersenne Twister Random algorithm that use to generate random numbers. To generate seeds, the `mt_srand()` function is utilized. The sequences generated with a specific seed may differ from PHP. Algorithm use the array data set from the slot row and shuffle each array row as much as random 1 to 5 times.

3.3 Scope of evaluation

The scope of evaluation of RNG is Level 1 testing against Curaçao eGaming GLI 19.

3.4 Conclusions and Recommendations

The current implementation of Global Games RNG complies with the requirements of Curaçao eGaming compliance against Chapter 3: Random Number Generator (RNG) Requirements of GLI-19: Standards.

ga concludes and recommends that the current implementation of the Global Games pRNG is suitable for use in online games and meets Curaçao eGaming requirements.

4 Test Results

This section summarises the results of the tests performed on Global Game Internusa B.V RNG. The tables in the following sub-sections provide the compliance status of the RNG for Curaçao eGaming against GLI 19 RNG requirements listed in [1]. Different values used in the compliance status column are described as follows:

Comply: The RNG complies with the requirement.

Pending: The requirement could not be verified at the time of RNG evaluation.

Acknowledged: The requirement is only a statement or information.

N/A: The requirement is not applicable to the RNG.

Out of scope: The requirement cannot be evaluated at this stage due to the current scope of testing or limitation of test environment.

4.1 Chapter 3: Random Number Generator (RNG) Requirements

Article	GLI - 19 Requirements	Compliance Status	Comments/Notes
Chapter 3:	Random Number Generator (RNG) Requirements		
3.1	Introduction		
3.1.1	General Statement		
	This chapter sets forth the technical requirements for a Random Number Generator (RNG). The types of RNGs include the following:	Acknowledged	
	a) Software-based RNGs do not use hardware devices and derive their randomness principally and primarily from a computer-based or software-driven algorithm. They do not incorporate hardware randomness in a significant way.	Comply	The random numbers are generated by using PHP with the implementation of Mersenne Twister Random algorithm. The data generated from the RNG is random
	b) Hardware-based RNGs derive their randomness from small-scale physical events (e.g., electric circuit feedback, thermal noise, radioactive decay, photon spin, etc.).	N/A	
	c) Mechanical RNGs generate game outcomes mechanically, employing the laws of physics (e.g., wheels, tumblers, blowers, shufflers, etc.).	N/A	This is a Software-based RNG.
	NOTE: See also related requirements found in “Game Outcome Using a Random Number Generator” section as contained in the “Game Requirements” chapter of this standard.	Acknowledged	
3.2	General RNG Requirements		
3.2.1	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. This review shall include comparison to published references, where applicable, and an examination for sources of bias, errors in implementation, malicious code, code with the potential to corrupt behavior, or undisclosed switches or parameters having a possible influence on randomness and fair play.	Comply	It has been verified, through source code review the data generated from the RNG is random and fair.
3.2.2	Statistical Analysis		

Article	GLI - 19 Requirements	Compliance Status	Comments/Notes
	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”). 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. 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. The applied tests shall be evaluated, collectively, at a 99% confidence level. 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. Statistical tests may include any one or more of the following: a) Total Distribution or Chi-square test; b) Overlaps test; c) Coupon Collector's test; d) Runs test; e) Interplay Correlation test; f) Serial Correlation test; and g) Duplicates test.	Comply	It has been verified, through statistical analysis, that the data are statistically independent and the data output of pRNG passed statistical tests. See Annex A: Statistical testing of RNG output.
3.2.3	Distribution		
	Each possible RNG selection shall be equally likely to be chosen. Where the game design specifies a non-uniform distribution, the final outcome shall conform to the intended distribution.	Acknowledged	
	a) 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.	Comply	It has been verified, through source code review the data generated from the RNG is random and fair.
	b) The final outcome output shall be tested against intended distribution using appropriate statistical tests (e.g., Total Distribution test).	Comply	It has been verified through statistical analysis that the scaled numbers are random and uniformly distributed over the range required. See Annex A: Statistical testing of RNG output.
3.2.4	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.	Acknowledged	
	a) 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).	Comply	It has been verified, through source code review, that RNG cannot reproduce a previous output stream.
	b) 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).	Comply	The data is statistically independent and the data output of pRNG passed statistical tests. See Annex A: Statistical testing of RNG output.

Article	GLI - 19 Requirements	Compliance Status	Comments/Notes
3.2.5	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.	Comply	The RNG cannot reproduce a previous output stream. It is very unlikely that two instances of pRNG produce the same stream.
3.3	RNG Strength and Monitoring		
3.3.1	RNG Strength for Outcome Determination		
	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.	Comply	
3.3.2	Cryptographic RNG Attacks		
	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:	Acknowledged	
	a) 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 shall be ensured through the appropriate use of a recognized cryptographic algorithm (RNG algorithm, hash, cipher, etc.). Note that a hardware-based RNG or a mechanical RNGs may potentially qualify as a cryptographic algorithm, provided it passes statistical testing;	Comply	The random numbers are generated by using PHP with the implementation of Mersenne Twister Random algorithm which is cryptographically secure. See Annex A: Statistical testing of RNG output.
	b) 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 shall not be seeded from a time value alone. The manufacturer shall ensure that games will not have the same initial seed.	Comply	
	Seeding methods shall not compromise the cryptographic strength of the RNG; and	Comply	Seeding and re-seeding does not introduce any predictability as the seeding based on the mt_srand() function.
	c) 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.	N/A	
	NOTE: Because of continuous computational improvements and advances in cryptographic research, compliance to this criterion shall be re-evaluated as required by the regulatory body.	Acknowledged	
3.3.3	Dynamic Output Monitoring for Hardware-Based RNGs	N/A	
	Due to their physical nature, the performance of hardware-based RNGs may deteriorate over time or otherwise malfunction, independent of the Gaming 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		

Article	GLI - 19 Requirements	Compliance Status	Comments/Notes
	disable game play when malfunction or degradation is detected.		
3.4	Mechanical RNG (Physical Randomness Device)	N/A	
3.4.1	General Statement		
	The requirements defined within this section apply to mechanical RNGs or “physical randomness devices”. While software may be a part of the device, the software is primarily limited to operating machinery and/or reading and recording game outcome data (the software does not play a deterministic role in determining the game outcome).		
	NOTE: Devices which faithfully and mechanically create or display a game outcome selected by a computer RNG are not considered physical randomness devices and shall be tested as RNGs once the faithful reproduction of RNG selected outcome has been assured. Physical randomness devices may incorporate RNGs in secondary roles (e.g., rotation speed). Such secondary RNGs need not be evaluated against the RNG requirements contained herein, as they do not directly select the game outcome. Rather, the physical randomness device shall be tested as a whole as described in this section.		
	NOTE: The approved components of a physical randomness devices cannot be swapped out or replaced with unapproved components, as they are integral to the behavior and performance of the physical randomness devices. The “approved components” in this context include those physical items that produce the random behavior – e.g., balls in a mixer, cards in a shuffler, etc. As one example, a shuffler certified by the independent test laboratory to utilize plastic cards cannot be viewed as an approved equivalent to the same mechanical shuffler using paper cards.		
3.4.2	Data Collection		
	To provide best assurance of random behavior, the independent test laboratory shall collect game outcome data for at least 10,000 game outcomes. 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.		
	NOTE: Due to feasibility concerns associated with reasonable data collection on some devices, the regulatory body may elect to accept testing results from a smaller collection amount on a case-by-case basis. Equally possible, a larger data collection sample may be required. Regardless, the independent test laboratory will clearly state in the applicable certification, the amount of data used for testing. When less than 10,000 games are used, a statement on the statistical limitations of reduced testing will be clearly denoted within the certification report.		
3.4.3	Durability		

Article	GLI - 19 Requirements	Compliance Status	Comments/Notes
	All mechanical pieces shall be constructed of materials to prevent degradation of any component over its intended lifespan.		
	NOTE: The independent test laboratory may recommend a stricter replacement schedule than that suggested by the manufacturer of the device to comply with the 'Durability' requirement stated above. In addition, the independent test laboratory may recommend periodic inspection of the device to ensure and maintain its integrity.		
3.4.4	Tampering		
	The players and/or gaming attendants (e.g., dealers, croupiers, etc.) used in live games shall not have the ability to manipulate or influence the physical randomness devices in a physical manner with respect to the production of game outcome data, except as intended by game design.		

5 References

1. GLI-19: Standards for Interactive Gaming System Version: 3.0.
2. RNG Description “rng.docx”, no version, no date.

Annex A : Statistical testing of raw pRNG output

Statistical analysis of RNG output has been performed for:

- ♠ Raw (binary) RNG output; and
- ♠ Scaled RNG output for games served by the RNG.

This section provides results of the statistical analysis.

A.1 Diehard test results

Following table presents the summary of diehard test results. These tests were applied on raw output of RNG generated by the test harness provided by Global Game Internusa B.V. The data has passed the tests in the diehard battery of tests with 99% confidence interval.

Data file: Result1.txt

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0. 412857	Pass
2	BINARY RANK TEST for 31x31 matrices	0. 451397	Pass
3	BINARY RANK TEST for 32x32 matrices	0. 603934	Pass
4	BINARY RANK TEST for 6x8 matrices	0. 816382	Pass
5	BITSTREAM TEST	0. 485630	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0. 494093	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0. 421614	Pass
8	DNA test	0. 494093	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2467.23 chi-square value	0. 321543	Pass
	(ii) byte stream for 2444.43 chi-square value	0. 215951	Pass
10	COUNT-THE-1's TEST for specific bytes	0. 547901	Pass
11	PARKING LOT TEST	0. 462263	Pass
12	MINIMUM DISTANCE TEST	0. 965296	Pass
13	3DSPHERES TEST	0. 465558	Pass
14	SQUEEZE TEST	0. 082123	Pass
15	OVERLAPPING SUMS test	0. 222336	Pass
16	THE RUN TEST		
	(i) Runs up Test	0. 347580	Pass
	(ii) Runs Down Test	0. 776647	Pass
	(iii) Runs up Test	0. 042771	Pass
	(iv) Runs Down Test	0. 573558	Pass
17	CRAPS TEST		
	(i) No. of wins	0. 749054	Pass
	(ii) for throws/game	0. 474691	Pass

Test No.	Description	p-value	Test results (Pass/Fail)
18	OVERLAPPING 5-PERMUTATION TEST		
	(i) Sample of 1,000,000 consecutive 5-tuples	0. 289256	Pass
	(ii) Sample of 1,000,000 consecutive 5-tuples	0. 239262	Pass

Data file: Result2.txt

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0.060068	Pass
2	BINARY RANK TEST for 31x31 matrices	0. 347728	Pass
3	BINARY RANK TEST for 32x32 matrices	0. 824671	Pass
4	BINARY RANK TEST for 6x8 matrices	0. 436700	Pass
5	BITSTREAM TEST	0. 508174	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0. 409839	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0. 492725	Pass
8	DNA test	0. 417493	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2721.48 chi-square value	0. 999133	Pass
	(ii) byte stream for 2557.02 chi-square value	0. 789994	Pass
10	COUNT-THE-1's TEST for specific bytes	0. 524554	Pass
11	PARKING LOT TEST	0. 353931	Pass
12	MINIMUM DISTANCE TEST	0. 674720	Pass
13	3DSPHERES TEST	0. 204185	Pass
14	SQUEEZE TEST	0. 789699	Pass
15	OVERLAPPING SUMS test	0. 345440	Pass
16	THE RUN TEST		
	(i) Runs up Test	0. 763647	Pass
	(ii) Runs Down Test	0. 748272	Pass
	(iii) Runs up Test	0. 141807	Pass
	(iv) Runs Down Test	0. 088761	Pass
17	CRAPS TEST		
	(i) No. of wins	0. 699833	Pass
	(ii) for throws/game	0. 079445	Pass
18	OVERLAPPING 5-PERMUTATION TEST		
	(i) Sample of 1,000,000 consecutive 5-tuples	0. 054534	Pass
	(ii) Sample of 1,000,000 consecutive 5-tuples	0. 301136	Pass

A.2 Scaled data statistical testing results

The following tables describe the results of statistical testing performed on scaled data used to generate game results. The scaled data was generated using the RNG being evaluated.

The data passed all statistical tests within 99% confidence interval which confirms that the game outcomes are random and uniformly distributed over the range required by the games.

Data file name: 1scale.RES (Scaling range: 0 to 114)

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	1.1023e+002	Pass
Runs-up	10,000,000	3.5182e-004	Pass
Runs-down	10,000,000	3.3545e-004	Pass

Data file name: 2scale.RES (Scaling range: 0 to 114)

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	1.2910e+002	Pass
Runs-up	10,000,000	3.4996e-004	Pass
Runs-down	10,000,000	3.3177e-004	Pass
Correlation Test	10,000,000	-1.6324e-004	Pass

Annex C: Hashes of RNG

The following hashes of critical components for the product tested are recorded.

Name	Critical File Name	Version	Description	SHA-1 hashes
RNG	NSlot.php	V2.0.0	Class function for seeding and random value of number for get new slot set when user click spin.	SHA-1: a4e73197a702a24d4159ba6ca29dd5885a9a2271 SHA-256 9aa3df7ecd74166e502ceda9c7ca15768f928e376f8cb28885a76f0e56105a8e
	NSlotEnc.php	V2.0.0	This is encryption version of Nslot.php Class function for seeding and random value of number for get new slot set when user click spin.	SHA-1: 0b2ec43fa0f7c6dff0c4dcb30604a828028ae09d SHA-256 5554ced6763b3ffb04d0cf4c18859e7f4fea8cb694566bdca9aa35f738be3ab6



End of document