

Certification Report. Uniquent Limited RNG Evaluation

Report Identification UQH-MT-220902-01-RC-R1

Certification Laboratory



Gaming Associates Europe Ltd.
www.gamingassociates.com

- 178 Merton High Street,
London SW19 1AY,
United Kingdom.
- Office 7, 82 London Road
Leicester LE2 0QR
United Kingdom.
- 123, Melita Street
Valletta VLT 1123
Malta.

Supervisor: Usman Vaseer

Signatures:

Certifier: Wajahat Kashan

Dates of certification work: 05 August 2022 to 24 August 2022

Date of issue of certification report: 02 September 2022

Report prepared for: Uniquent Limited
 Address: 7 Archaias Ledras,
 Geri 2200 Nicosia,
 Cyprus

Register Number HE430701

Jurisdiction: Malta Gaming Authority, Malta

Technical Standard used for testing: Remote Gaming Regulations, 20 April 2005,
 Legal Notice 176 of 2004 of the Lotteries and other
 Games Act (ACT XXIV OF 2001) as amended by
 Legal Notices 110 of 2006, 270 and 426 of 2007, 90
 of 2011 and 131 of 2016



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 Ltd (hereinafter referred to as Gaming Associates or **ga**). Unauthorized copying and distribution of the documents, by any means, on any media is 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 it has discovered throughout the assessment period of the client's RNG related to the technical scope of testing as per applicable jurisdictional requirements. Results are based on the client's submission of information material, source code, and access to the testing environment, and applicable testing is performed within a finite period.

Inherently there are limitations in performing compliance testing within a laboratory environment and accordingly, **ga** has undertaken its best endeavours to ensure a thorough assessment is performed and a 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	Deriving game symbols and events	5
5	References.....	6
	Statistical testing of raw pRNG output.....	7
	Annex B: Statistical testing results of scaled data.....	10
	Annex C: Hashes of RNG source code and binary	11
	End of document.....	12

2.2 Version

Version	Description	Date
V0.1	Initial draft – MARB	2022-08-25
V0.2	Reviewed & Updated – WKAS	2022-08-26
V0.3	QA – UVAS	2022-08-29
V1.0	Final report to Uniquent	2022-09-02



3 Executive summary

3.1 Introduction

Uniquent Limited (Uniquent) has requested Gaming Associates (**ga**) to evaluate their pseudo-Random Number Generator (pRNG), also referred to as RNG in this report, being used in online gaming application against Malta Gaming Authority (MGA) Remote Gaming Regulations.

This report presents the results of evaluation performed by **ga** for the pRNG against MGA technical standards. Hashes of source code and binary files related to the pRNG are listed in Annex C of this report.

3.2 RNG details

Uniquent implemented servers run on Debian GNU/Linux 10 (buster) OS using PHP 8.0.7 version as scripting language. RNG is executed through use random_int function, /dev/urandom is cryptographically secure pseudo random number generator that provides thread safe random numbers. The /dev/urandom doesn't have a configurable seed option; rather it has an entropy pool where all available random information is stored. /dev/urandom constantly reseeding using all the available source for the entropy pool.

3.3 Scope of evaluation

The scope of evaluation of RNG testing against Malta Gaming Regulations.

3.4 Conclusions and Recommendations

The current implementation of Uniquent RNG complies with the requirements of MGA Remote Gaming Regulations.

ga concludes and recommends that the current implementation of the Uniquent RNG is suitable for use in Uniquent's gaming application and meets Malta Gaming Authority (MGA) RNG requirements.

4 Test Results

This section summarises the results of the tests performed on Uniquent Limited (Uniquent) pRNG. The tables in the following sub-sections provide the compliance status of the pRNG against MGA RNG requirements listed in [1]. Different values used in the compliance status column are described as follows:

Comply: The pRNG complies with the requirement.

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

Acknowledged: The requirement is only a statement or information.

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

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 Deriving game symbols and events

LGA Requirements	System Compliance	Comments/Anomalies
(3) the gaming system must satisfy the following criteria for randomness following Schneier:		
(a) the data must be randomly generated, passing appropriate statistical tests of randomness;	Comply	Uniquent is using PHP 8.0.7 version. Instance of /dev/urandom is cryptographically secure pseudo random number generator. The raw data output of pRNG passed statistical tests demonstrating that the data is statistically independent. Scaled data passed the statistical tests.
(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;	Comply	Uniquent pRNG use the /dev/urandom and it doesn't have a configurable seed option; rather it has an entropy pool where all available random information is stored. /dev/urandom constantly reseeding using all the available sources for the entropy pool.
(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.	Comply	The random numbers generated by Uniquent pRNG cannot be reproduced without the knowledge of the algorithm, its implementation, and the current seed value.

5 References

1. Remote Gaming Regulations, 20 April 2005, Legal Notice 176 of 2004 of the Lotteries and other Games Act (ACT XXIV OF 2001) as amended by Legal Notices 110 of 2006, 270 and 426 of 2007, 90 of 2011 and 131 of 2016
2. RNG Description “RNG doc-2.docx” no version, no date.



Annex A : Statistical testing of raw pRNG output

Statistical analysis of pRNG output has been performed for:

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

Following table presents the summary of diehard test results. These tests were applied on raw output of pRNG generated by the test harness provided by Uniquent Limited (Uniquent). The data has passed the tests in the diehard battery of tests with 99% confidence interval.

Data file: rand_1.bin

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0.142164	Pass
2	BINARY RANK TEST for 31x31 matrices	0.445841	Pass
3	BINARY RANK TEST for 32x32 matrices	0.933015	Pass
4	BINARY RANK TEST for 6x8 matrices	0.955622	Pass
5	BITSTREAM TEST	0.429554	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0.378347	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0.397342	Pass
8	DNA test	0.4976	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2488.44 chi-square value	0.435068	Pass
	(ii) byte stream for 2455.42 chi-square value	0.264220	Pass
10	COUNT-THE-1's TEST for specific bytes	0.494539	Pass
11	PARKING LOT TEST	0.647189	Pass
12	MINIMUM DISTANCE TEST	0.147405	Pass
13	3DSPHERES TEST	0.892286	Pass
14	SQUEEZE TEST	0.617621	Pass
15	OVERLAPPING SUMS test	0.567025	Pass
16	THE RUN TEST		
	(i) Runs up Test	0.698186	Pass
	(ii) Runs Down Test	0.452953	Pass
	(iii) Runs up Test	0.461685	Pass
	(iv) Runs Down Test	0.663809	Pass
17	CRAPS TEST		
	(i) No. of wins	0.319538	Pass
	(ii) for throws/game	0.122708	Pass



Test No.	Description	p-value	Test results (Pass/Fail)
18	OVERLAPPING 5-PERMUTATION TEST		
	(i) Sample of 1,000,000 consecutive 5-tuples	0.125056	Pass
	(ii) Sample of 1,000,000 consecutive 5-tuples	0.139448	Pass

Data file: rand_2.bin

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0.866298	Pass
2	BINARY RANK TEST for 31x31 matrices	0.497306	Pass
3	BINARY RANK TEST for 32x32 matrices	0.587318	Pass
4	BINARY RANK TEST for 6x8 matrices	0.574062	Pass
5	BITSTREAM TEST	0.482785	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0.552986	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0.552025	Pass
8	DNA test	0.504225	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2412.44 chi-square value	0.107795	Pass
	(ii) byte stream for 2555.94 chi-square value	0.785570	Pass
10	COUNT-THE-1's TEST for specific bytes	0.498691	Pass
11	PARKING LOT TEST	0.351011	Pass
12	MINIMUM DISTANCE TEST	0.967044	Pass
13	3DSPHERES TEST	0.600693	Pass
14	SQUEEZE TEST	0.402084	Pass
15	OVERLAPPING SUMS test	0.610149	Pass
16	THE RUN TEST		
	(i) Runs up Test	0.392694	Pass
	(ii) Runs Down Test	0.724117	Pass
	(iii) Runs up Test	0.525332	Pass
	(iv) Runs Down Test	0.291272	Pass
17	CRAPS TEST		
	(i) No. of wins	0.249923	Pass
	(ii) for throws/game	0.407992	Pass



Test No.	Description	p-value	Test results (Pass/Fail)
18	OVERLAPPING 5-PERMUTATION TEST		
	(i) Sample of 1,000,000 consecutive 5-tuples	0.077415	Pass
	(ii) Sample of 1,000,000 consecutive 5-tuples	0.144920	Pass



Annex B : Statistical testing results of scaled data

The following table describes the results of statistical testing performed on scaled data used to generate games results. The scaled data was generated using the pRNG 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: rand_5.txt (Scaling range: 0 to 36)

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	3.3145e+001	Pass
Runs-up	10,000,000	2.3082e-003	Pass
Runs-down	10,000,000	2.2198e-003	Pass

Data file name: rand_6.txt (Scaling range: 0 to 36)

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	3.0388e+001	Pass
Runs-up	10,000,000	2.2422e-003	Pass
Runs-down	10,000,000	2.2877e-003	Pass
Correlation Test	10,000,000	-6.7273e-005	Pass

Data file name: rand_2.txt (Scaling range: 0 to 5000000)

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	5.0013e+006	Pass
Runs-up	10,000,000	1.5586e-004	Pass
Runs-down	10,000,000	1.5218e-004	Pass

Data file name: rand_3.txt (Scaling range: 0 to 5000000)

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	4.9972e+006	Pass
Runs-up	10,000,000	1.5258e-004	Pass
Runs-down	10,000,000	1.5352e-004	Pass
Correlation Test	10,000,000	6.8948e-005	Pass



Annex C : Hashes of RNG source code and binary

SHA-1 hashes of files related to the Uniquent Limited (Uniquent) pRNG have been taken to establish a baseline of the system evaluated by **ga**. The hashes are listed below.

Critical Components	SHA-1 Hashes
ReelSet.php	SHA-1 Hash: 60A0FAAE2DB52D58629327E79725151A9A089B7C SHA-256 Hash: CD6B809D620B28D85C346F363A7E40F09DE1365CF0B881754520F8A0B350BC5B
ReelProcessor.php	SHA-1 Hash: 63972E8D1E06AFE43776BB60915B2612DB1A16F SHA-256 Hash: 3179CE5E14D2A289B6FC6DB0D72169BD43751F95B087A7FB39E83965B35E0E51



End of document