



Certification Report: Ahnah Investment NV RNG Evaluation

Report Identification: AHI-CR-230202-01-RC-R1

Certification Laboratory:



Gaming Associates Europe Ltd. Stockholm, Sweden
www.gamingassociates.com

- 178 Merton High Street,
London, UK, SW19 1AY.
- Office 7, 82 London Road
Leicester, UK, LE2 0QR
- Hamngatan 27,

Supervisor: Usman Vaseer

Signatures:

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

Certifier: Wajahat kashan

Dates of certification work: 25 January 2023 to 02 February 2023

Date of issue of certification report: February 02, 2023

Report prepared for: Ahnah Investment NV
Abraham de Veerstraat 9,
Curacao

Jurisdiction: Curaçao eGaming

Technical Standard used for testing: UK Remote Gambling and Software Technical Standards, February 2021



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 (**ga**) Company No. 9663955. Unauthorised 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 document is for Ahnah Investment NV and Curaçao eGaming to advise the compliance status Ahnah Investment NV pRNG, against UKGC Remote Gambling and Software Technical Standards, February 2021.

The documents are copyright.

1.2 Disclaimer

Ga has reported on what it has discovered through evaluation of Ahnah Investment NV pRNG. This report is not an evaluation of the game or interactive gaming system and related processes.



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	Conclusions and Recommendations	4
4	Test Results	5
4.1	RTS 7 – Generation of random outcomes	5
	References.....	8
	Annex A : Statistical testing of raw pRNG output.....	9
A.1	Diehard test results.....	9
	Annex B: Statistical testing results of scaled data.....	14
B.1.1	Statistical testing results	14
	Annex C: Hashes of RNG	17
	End of document.....	18

2.2 Version

Version	Description	Date
V0.1	Initial draft –WKAS	2023-01-26
V1.0	QA & release – UVAS	2023-02-02



3 Executive summary

3.1 Introduction

Ahnah Investment NV has requested Gaming Associates (**ga**) to evaluate their pseudo Random Number Generator (pRNG) being used in online games for Curaçao eGaming against UK (UKGC) Remote Gambling and Software Technical Standards (RTS), February 2021 [1].

This report presents the results of evaluation performed by **ga** for the pRNG for Curaçao eGaming against UKGC 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

Ahnah Investment NV is using SH-256 algorithm to generate the pseudorandom numbers with using the node crypto library.

3.3 Conclusions and Recommendations

The current implementation of Ahnah Investment NV pRNG complies with the requirements of Curaçao eGaming compliance against UKGC Remote Gambling and Software Technical Standards, February 2021.

Ga concludes and recommends that the current implementation of the Ahnah Investment NV 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 Ahnah Investment NV pRNG. The tables in the following sub-sections provide the compliance status of the pRNG for Curaçao eGaming against UKGC 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 RTS 7 – Generation of random outcomes

UKGC Requirements	System Compliance	Comments/Anomalies
Remote Technical Standards (RTS)		
RTS 7 – Generation of random outcomes		
Gaming (including bingo), lotteries, and betting on virtual events		
RTS aim 7		
To ensure that games and other virtual events operate fairly.		
RTS requirement 7A		
Random number generation and game results must be 'acceptably random'. Acceptably random here means that it is possible to demonstrate to a high degree of confidence that the output of the RNG, game, lottery and virtual event outcomes are random through, for example, statistical analysis using generally accepted tests and methods of analysis. Adaptive behaviour (i.e. a compensated game) is not permitted.	Comply	Ahnah Investment NV is using SH-256 algorithm to generate the pseudorandom numbers with using the node crypto library. See "Annex A: Statistical testing of raw pRNG output" and "Annex B: Statistical testing results of scaled data" for details.
Where lotteries use the outcome of other events, external to the lottery, to determine the result of the lottery (for example, using numbers from the National Lottery) the outcome must be unpredictable and externally verifiable.	N/A	Ahnah Investment NV does not rely on any external events.
RTS implementation guidance 7A		
a. Random number generators should be capable of demonstrating the following qualities:		
i. the output from the random number generator is uniformly distributed over the entire output range and game, lottery, or virtual event outcomes are distributed in accordance with the expected/theoretical probabilities;	Comply	It has been verified, through statistical analysis, that the scaled numbers generated from the pRNG are distributed in accordance with the expected probabilities for gameplay. See Annex B: Statistical testing results of scaled data.



UKGC Requirements	System Compliance	Comments/Anomalies
ii. the output of the RNG, game, lottery, and virtual event outcomes should be unpredictable, for example, for a software RNG it should be computationally infeasible to predict what the next number will be without complete knowledge of the algorithm and seed value;	Comply	The random numbers generated by pRNG cannot be predicted as it is seeded every time before generating a random number.
iii. random number generation does not reproduce the same output stream (cycle), and that two instances of a random number generator do not produce the same stream as each other (synchronise);	Comply	It is not likely that the pRNG will reproduce a previous output stream because seeding is based on random sources.
iv. any forms of seeding and re-seeding used do not introduce predictability; and	Comply	The pRNG is seeded every time numbers are required.
v. any scaling applied to the output of the random number generator maintains the qualities above.	Comply	It has been verified through statistical analysis that the scaled data. <i>See Annex B: Statistical testing results of scaled data.</i>
b. For lotteries using external events - where it is not practical to demonstrate a. above - the events outcomes should be:		
i. unpredictable, that is, events should be selected only where they may reasonably be assumed to be random events;	N/A	Ahnah Investment NV does not use outcomes of any external events.
ii. unable to be influenced by the lottery operator (or external lottery manager); and	N/A	Ahnah Investment NV does not use outcomes of any external events.
iii. publicly available and externally verifiable, for example, events that are published in local or national press would be acceptable.	N/A	Ahnah Investment NV does not use outcomes of any external events.
c. For games or virtual events that use the laws of physics to generate the outcome of the game (mechanical RNGs), the mechanical RNG used should be capable of meeting the requirements in a. where applicable and in addition:		
i. the mechanical pieces should be constructed of materials to prevent decomposition of any component over time (e.g. a ball shall not disintegrate);	N/A	Ahnah Investment NV does not use mechanical RNG.
ii. the properties of physical items used to choose the selection should not be altered; and	N/A	Ahnah Investment NV does not use mechanical RNG.
iii. players should not have the ability to interact with, come into physical contact with, or manipulate the mechanics of the game.	N/A	Ahnah Investment NV does not use mechanical RNG.
d. Restricting adaptive behaviour prohibits automatic or manual interventions that change the probabilities of game outcomes occurring during play. Restricting adaptive behaviour is not intended to prevent games from offering bonus or special features that implement a different set of rules, if they are based on the occurrence of random events.	N/A	Ahnah Investment NV does not have any adaptive behaviour in generating game results.
RTS requirement 7B		
As far as is reasonably possible, games and events must be implemented fairly and in accordance with the rules and prevailing payouts, where applicable, as they are described to the customer.	Comply	The current scope included verification of randomness of the results generated from pRNG. Verification of complete game rules and payouts is out of scope.



UKGC Requirements	System Compliance	Comments/Anomalies
RTS implementation guidance 7B		
a. Games should implement the rules as described in the rules available to the customer before play commenced.	Out of scope	The current scope included verification of randomness of the results generated from pRNG. Verification of complete game rules and payouts is out of scope.
b. The mapping of the random inputs to game outcomes should be in accordance with prevailing probabilities, pay tables, etc.	Out of scope	The current scope included verification of randomness of the results generated from pRNG. Verification of complete game rules and payouts is out of scope.
c. When random numbers, scaled or otherwise, are received, e.g. following a game requesting a sequence of random numbers, they are to be used in the order in which they are received. For example, they may not be discarded due to adaptive behaviour.	Comply	The pRNG provides scaled random numbers as requested by game and these numbers are used in the order they are received. No random numbers are discarded by the games.
d. Numbers or sequences of numbers are not to be discarded, unless they fall outside the expected range of numbers required by the virtual event – such an occurrence should result in an error being logged and investigated.	Comply	The pRNG provides scaled random numbers according to the range required by the game. The scaled numbers do not fall outside the expected range required by the games.



References

1. UKGC Remote Gambling and Software Technical Standards, February 2021



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.

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 pRNG generated by the test harness provided by Ahnah Investment NV. The data has passed majority of the tests in the diehard battery of tests. The pRNG is considered to have overall passed the diehard tests with 99% confidence interval.

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0. 158663	Pass
2	BINARY RANK TEST for 32x32 matrices	0. 597385	Pass
3	BINARY RANK TEST for 31x31 matrices	0. 973189	Pass
4	BINARY RANK TEST for 6x8 matrices	0. 274846	Pass
5	BITSTREAM TEST	0. 596383	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0. 492652	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0. 436603	Pass
8	DNA test	0. 476329	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2585.48 chi-square value	0. 886655	Pass
	(ii) byte stream for 2634.93 chi-square value	0. 971817	Pass
10	COUNT-THE-1's TEST for specific bytes	0. 586689	Pass
11	PARKING LOT TEST	0. 413737	Pass
12	MINIMUM DISTANCE TEST	0. 201539	Pass
13	3DSPHERES TEST	0. 612472	Pass
14	SQUEEZE TEST	0. 042711	Pass
15	OVERLAPPING SUMS test	0. 691781	Pass
16	THE RUN TEST		
	(i) Runs up Test	0. 926377	Pass
	(ii) Runs Down Test	0. 514773	Pass
	(iii) Runs up Test	0. 106011	Pass
	(iv) Runs Down Test	0. 069847	Pass



Test No.	Description	p-value	Test results (Pass/Fail)
17	CRAPS TEST		
	(i) No. of wins	0. 169409	Pass
	(ii) for throws/game	0. 945886	Pass
18	OVERLAPPING 5-PERMUTATION TEST		
	(i) Sample of 1,000,000 consecutive 5-tuples	0. 998960	Pass
	(ii) Sample of 1,000,000 consecutive 5-tuples	0. 941308	Pass

Result file: rb-2-out.txt

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0. 543323	Pass
2	BINARY RANK TEST for 32x32 matrices	0. 791492	Pass
3	BINARY RANK TEST for 31x31 matrices	0. 905314	Pass
4	BINARY RANK TEST for 6x8 matrices	0. 492906	Pass
5	BITSTREAM TEST	0. 367042	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0. 477569	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0. 58185	Pass
8	DNA test	0. 458267	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2547.11 chi-square value	0. 747373	Pass
	(ii) byte stream for 2514.01 chi-square value	0. 578548	Pass
10	COUNT-THE-1's TEST for specific bytes	0. 540824	Pass
11	PARKING LOT TEST	0. 387061	Pass
12	MINIMUM DISTANCE TEST	0. 180621	Pass
13	3DSPHERES TEST	0. 393471	Pass
14	SQUEEZE TEST	0. 677840	Pass
15	OVERLAPPING SUMS test	0. 105160	Pass
16	THE RUN TEST		
	(i) Runs up Test	0. 834861	Pass
	(ii) Runs Down Test	0. 398667	Pass
	(iii) Runs up Test	0. 603242	Pass
	(iv) Runs Down Test	0. 370342	Pass
17	CRAPS TEST		



Test No.	Description	p-value	Test results (Pass/Fail)
	(i) No. of wins	0.731661	Pass
	(ii) for throws/game	0.645177	Pass
18	OVERLAPPING 5-PERMUTATION TEST		
	(i) Sample of 1,000,000 consecutive 5-tuples	0.003820	Fail
	(ii) Sample of 1,000,000 consecutive 5-tuples	0.986246	Pass

Result file: rb-3-out.txt

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0.016288	Pass
2	BINARY RANK TEST for 32x32 matrices	0.647599	Pass
3	BINARY RANK TEST for 31x31 matrices	0.975583	Pass
4	BINARY RANK TEST for 6x8 matrices	0.176403	Pass
5	BITSTREAM TEST	0.465256	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0.545465	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0.516721	Pass
8	DNA test	0.498038	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2392.25 chi-square value	0.063772	Pass
	(ii) byte stream for 2525.22 chi-square value	0.639312	Pass
10	COUNT-THE-1's TEST for specific bytes	0.552200	Pass
11	PARKING LOT TEST	0.952540	Pass
12	MINIMUM DISTANCE TEST	0.749926	Pass
13	3DSPHERES TEST	0.263770	Pass
14	SQUEEZE TEST	0.074913	Pass
15	OVERLAPPING SUMS test	0.749241	Pass
16	THE RUN TEST		
	(i) Runs up Test	0.288359	Pass
	(ii) Runs Down Test	0.029806	Pass
	(iii) Runs up Test	0.984991	Pass
	(iv) Runs Down Test	0.271878	Pass
17	CRAPS TEST		
	(i) No. of wins	0.491330	Pass
	(ii) for throws/game	0.436760	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. 000005	Fail
	(ii) Sample of 1,000,000 consecutive 5-tuples	0. 029000	Pass

Result file: rb-4-out.txt

Test No.	Description	p-value	Test results (Pass/Fail)
1	BIRTHDAY SPACINGS TEST	0. 877922	Pass
2	BINARY RANK TEST for 32x32 matrices	0. 474772	Pass
3	BINARY RANK TEST for 31x31 matrices	0. 432456	Pass
4	BINARY RANK TEST for 6x8 matrices	0. 580916	Pass
5	BITSTREAM TEST	0. 494261	Pass
6	Overlapping Pairs-Sparse-Occupancy (OPSO) Test	0. 674013	Pass
7	Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test	0. 464585	Pass
8	DNA test	0. 529167	Pass
9	COUNT-THE-1's TEST		
	(i) byte stream for 2548.42 chi-square value	0. 753260	Pass
	(ii) byte stream for 2384.82 chi-square value	0. 051667	Pass
10	COUNT-THE-1's TEST for specific bytes	0. 624211	Pass
11	PARKING LOT TEST	0. 448883	Pass
12	MINIMUM DISTANCE TEST	0. 476890	Pass
13	3DSPHERES TEST	0. 489182	Pass
14	SQUEEZE TEST	0. 737636	Pass
15	OVERLAPPING SUMS test	0. 443716	Pass
16	THE RUN TEST		
	(i) Runs up Test	0. 524926	Pass
	(ii) Runs Down Test	0. 859003	Pass
	(iii) Runs up Test	0. 679032	Pass
	(iv) Runs Down Test	0. 574802	Pass
17	CRAPS TEST		
	(i) No. of wins	0. 049041	Pass
	(ii) for throws/game	0. 642039	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. 578705	Pass
	(ii) Sample of 1,000,000 consecutive 5-tuples	0. 005071	Fail



Annex B: Statistical testing results of scaled data

B.1.1 Statistical testing results

The following tables describes the results of statistical testing performed on scaled data used to generate game results. The scaled data was generated using the same pRNG which is deployed in the production systems.

The data passed all statistical tests within 99% confidence interval which are accepted standard intervals for statistical tests of this nature. This confirms that the game outcomes are random and uniformly distributed over the range required by the games.

Scaled 1A

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	3.0218e+001	Pass
Runs-up	10,000,000	4.9028e-003	Pass
Runs-down	10,000,000	4.8973e-003	Pass

Scaled 1B

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	51,708,342	2.2376e+001	Pass
Runs-up	51,708,342	4.8501e-003	Pass
Runs-down	51,708,342	4.8637e-003	Pass

Correlation between both files:

Sampling size	correlation coefficient	Pass/Fail
10,000,000	3.9412e-005	Pass

Scaled 2A

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	2.5771e+001	Pass
Runs-up	10,000,000	2.2487e-003	Pass
Runs-down	10,000,000	2.2597e-003	Pass

Scaled 2B

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	2.2944e+001	Pass
Runs-up	10,000,000	2.2587e-003	Pass
Runs-down	10,000,000	2.2679e-003	Pass



Correlation between both files:

Sampling size	correlation coefficient	Pass/Fail
10,000,000	1.4387e-004	Pass

Scaled 3A

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	3.3188e+001	Pass
Runs-up	10,000,000	1.9594e-003	Pass
Runs-down	10,000,000	1.9404e-003	Pass

Scaled 3B

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	100,000,000	4.9837e+001	Pass
Runs-up	100,000,000	1.9306e-003	Pass
Runs-down	100,000,000	1.9730e-003	Pass

Correlation between both files:

Sampling size	correlation coefficient	Pass/Fail
10,000,000	-1.7589e-004	Pass

Scaled 4A

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	7.6791e+001	Pass
Runs-up	10,000,000	1.1950e-003	Pass
Runs-down	10,000,000	1.2050e-003	Pass

Scaled 4B

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	4.2718e+001	Pass
Runs-up	10,000,000	1.2026e-003	Pass
Runs-down	10,000,000	1.2050e-003	Pass

Correlation between both files:

Sampling size	correlation coefficient	Pass/Fail
10,000,000	1.4387e-004	Pass



Scaled 5A

Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
Chi-Square	10,000,000	9.8055e+004	Pass
Runs-up	10,000,000	4.0593e-004	Pass
Runs-down	10,000,000	4.2089e-004	Pass

Scaled 5B

DOF	Data File	Statistical test	Sampling size	Sum of square of residuals	Pass/Fail
100	Dice.dump	Chi-Square	100,000,000	9.8011e+005	Pass
		Runs-up	100,000,000	4.1346e-004	Pass
		Runs-down	100,000,000	4.1111e-004	Pass

Correlation between both files.

Sampling size	correlation coefficient	Pass/Fail
10,000,000	4.8460e-006	Pass



Annex C: Hashes of RNG

SHA1 hashes for the RNG files are listed below:

Version: 1.0.0 +

Rand.php	1608b15f28f628e3e0b6f159b02acf0be15ca5cb
----------	--

Version: 1.1+

Rand.php	946859971359EB73BE27DDEE11F9D4253E8BA633
----------	--



End of document