



eCOGRA LIMITED

MALTA GAMING AUTHORITY

**RANDOMNESS EVALUATION REPORT
RANDOM NUMBER GENERATOR**

FOR

HGMT LTD

REPORT REFERENCE NUMBER: e228356HCKMLT

REPORT ISSUE DATE: 20 JUNE 2022

CONFIDENTIAL

IMPORTANT DISCLAIMER

This report is supplied on the basis that it is for the sole use of the parties listed and to whom it is addressed, and exclusively for the objectives set out herein.

No party, other than those specified, may rely on this report for any purpose whatsoever.

eCOGRA Limited ('eCOGRA') does not accept any liability or responsibility towards any third party to whom this report is shown or into whose hands it may fall.

This report should not be relied upon for any assurances in relation to third parties and/or activities which are not covered by the certifiable regulatory requirements or compliance standards of the jurisdiction, regulatory authority or compliance entity or system for whose purposes this report is stated to have been prepared. All such other parties and activities are outside the scope of this report and have therefore not been reviewed by eCOGRA.

The nature, timing and extent of testing conducted for the purpose of the certification is considered sufficient and appropriate based on the applicable certifiable regulations and professional judgement applied to the associated risk of non-compliance. The certification of compliance should not be construed to imply any warranty over the functionality, quality or performance of the subject of certification. eCOGRA reserves the right to withdraw this certificate if any non-compliances are subsequently detected by or reported to eCOGRA.

CONFIDENTIALITY NOTICE

This document is proprietary to eCOGRA and contains confidential information of commercial value to eCOGRA, the disclosure of which to third parties could adversely affect the business affairs of eCOGRA.

This information is supplied in confidence to you, on the strict condition that no part of it is disclosed to any third party, in particular to any person or organisation that may be in competition with eCOGRA without the prior written approval of eCOGRA.

TABLE OF CONTENTS

TABLE OF CONTENTS	3
SECTION 1. INTRODUCTION	4
SECTION 2. GENERAL INFORMATION	4
SECTION 3. SOFTWARE DETAILS	6
SECTION 4. ASSESSMENT RESULTS.....	7
SCHEDULE 1. RNG TESTING	9
1. TESTS PERFORMED.....	9
2. TEST RESULTS	10

SECTION 1. INTRODUCTION

HGMT Ltd requested eCOGRA to evaluate the randomness of the Random Number Generator (RNG) to be utilised for the offering of online gambling products against the relevant regulatory requirements for the jurisdiction as listed below. The Random Number Generator used for the gambling applications is Software based.

SECTION 2. GENERAL INFORMATION

CLIENT NAME:	HGMT Ltd
CLIENT ADDRESS:	1ST FLOOR, SUITE 3, CENTRAL BUSINESS CENTRE, MDINA ROAD, ZEBBUG, ZBG 9015, MALTA
CLIENT CONTACT PERSON:	Daniel Camilleri
CLIENT E-MAIL ADDRESS:	daniel@hacksawgaming.com
CLIENT TELEPHONE NUMBER/SKYPE:	+46731050000
PRODUCT NAME:	Hacksaw Gaming - Random Number Generator
SUPPLIER:	HGMT Ltd
PRODUCT DESCRIPTION:	The RNG is a small wrapper around the system's cryptographic RNG capabilities. The wrapper code is implemented in C#.
PRODUCT VERSION:	1.0.5
RNG TYPE:	Software
JURISDICTION:	Malta
ASSESSMENT STANDARDS AND CRITERIA:	Licensing requirements of the Malta Gaming Authority ('MGA') Subsidiary Legislation 438.04 Remote Gaming Regulations Third Schedule, Regulation 25.
ACCREDITED BODY FULL NAME:	eCOGRA Limited
ACCREDITED BODY LEGAL FORM:	Private Company
ACCREDITED BODY MANAGING ADDRESS:	2 nd Floor Berkeley Square House, Berkeley Square, London, W1J 6BD, United Kingdom
ACCREDITED BODY ACCREDITATIONS HELD:	An Accredited Testing Body No. 4656. ISO/IEC 17025:2017, Issued by The United Kingdom Accreditation Service (Issue: 028, Issue Date: 10 May 2022).

ACCREDITED BODY EXPERIENCE:	19 years' testing and inspection of Online Gambling Systems; 6 years' auditing and certifying Information Security Management Systems; 7 years' of Risk and Vulnerability analyses.
ACCREDITED BODY REPRESENTATIVE:	Bradley Khoury
ACCREDITED BODY CONTACT EMAIL:	info@ecogra.org
ACCREDITED BODY CONTACT NUMBER:	Tel: +44 20 7887 1480
DATE OF TESTING AND INSPECTION:	09 June 2022 - 20 June 2022
PLACE OF TESTING:	The Accredited Body's premises.
REPORT TYPE:	Randomness Evaluation Report
REPORT REFERENCE NUMBER:	e228356HCKMLT
REPORT ISSUE DATE:	20 June 2022
ASSESSMENT RESULT:	Compliant
ACCREDITED BODY REPORT APPROVAL:	

A handwritten signature in black ink, appearing to be "B. Khoury", written over a horizontal line.

Bradley Khoury
Chief Technical Officer and Director

SECTION 3. SOFTWARE DETAILS

The scope of the RNG evaluation and certification applies solely to the files, file versions and associated hashes provided in the tables below:

File Name	Version	Digital Signature (SHA1 Hash)
HacksawGaming.RNG.dll	1.0.5	C3C2A3291ADB3B95DF0E9755102A28EDD71B6C27

SECTION 4. ASSESSMENT RESULTS

Testing procedures were performed against certifiable sections of the following laws and regulations of Malta Gaming Authority, as applicable to the components relevant to the products within scope:

- Licensing requirements of the Malta Gaming Authority ('MGA')
Subsidiary Legislation 438.04
Remote Gaming Regulations
Third Schedule, Regulation 25

Different values used in the "Assessment Result" column is described as follows:

- **Compliant:** The components within the assessment scope conform to the assessment standards and criteria.
- **Not Applicable:** The requirement is not applicable for the assessment of conformance. Refer to comments for further information.
- **Out of Scope:** The requirement for the assessment of conformance cannot be evaluated at this stage due to the current scope of testing/inspection or limitation of the test/inspection environment. Refer to comments for further information.
- **Compliant with Observation:** The components within the assessment scope conform to the assessment standards and criteria with certain limitations or an area of moderate risk of potential non-compliance identified. Refer to comments for further information.

Remote Gaming Regulations Third Schedule, Regulation 25 - Technical requirement for gaming system			
Requirement No.	Requirement Assessed	Assessment Result	Comments
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; 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; 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.	Compliant	The compliance assessment is based on a limited scope of testing which includes the assessment of the RNG as a standalone component without integration with any games. Further testing may be required in individual game assessments to validate full compliance of this requirement for each applicable game.

SCHEDULE 1. RNG TESTING

1. TESTS PERFORMED

An overview of the assessment approach of the Random Number Generator (RNG) is outlined below. We evaluated the RNG to ensure that it meets the relevant certifiable requirements. The scope of the evaluation consisted of an assessment of the following aspects:

Documentation	The RNG documentation is reviewed to allow for understanding the implementation of the RNG in the gaming system. Research is conducted on the RNG algorithm/hardware to ensure that there are no widely known weaknesses within the RNG under review.
Functionality	This involves an understanding of how random numbers received, following a call to the RNG requesting a sequence of random numbers, and how they are used. They must be used in the order in which they are received.
Source Code	The source code is reviewed to ensure that the implementation of the RNG is in accordance with the RNG documentation provided by the client. A walkthrough is conducted to show the nature of calls to the RNG as well as how the results are utilised.
Seeding and Reseeding	This involves gaining an understanding of the norms of initialisation of the RNG, including seeding sources which are verifiable sources of entropy. The seeding and reseeding used should not introduce predictability.
Mapping and Scaling	Any scaling applied to the output of the random number generator maintains uniform distribution over the entire output range. It should be ensured that game event outcomes are distributed in accordance with the expected/theoretical probabilities.
Security of RNG	Understanding the security of generated numbers during transmission between the RNG server and the gaming server.
Monitoring of RNG	Understanding the systems in place to monitor functionality of the RNG during live use, with the purpose of identifying early detection of irregularities in RNG output.
Cryptographic Strength	Review published documentation on the RNG algorithm. Evaluation of the algorithm, period length and seeding/re-seeding characteristics of the RNG and established that it contains features associated with cryptographically strong RNGs to ensure the sequence of random values generated cannot be predicted or reliably reproduced.

Test Suites	The test suite used to perform the evaluation consisted of the following: • Chi-Squared Tests; • Wald-Wolfowitz (or Runs) Tests; • Correlation and Serial Correlation; • Expected probabilities for shuffle decks; and • Diehard Test Suite. Process and analyse six sets of output generated data logs (180 files) consisting of scaled ranges, shuffled decks and hexadecimal values for Diehard Test Suite. Application of numerous mathematical and statistical tests to verify: • the variation in the data is due to random chance; • the results are within the acceptable parameters to demonstrate statistical independence; • the results calculate the correct standard deviations from their expected values; and • the results of the output values are unpredictable.
--------------------	--

2. TEST RESULTS

Recognised statistical and mathematical tests were performed to certify the RNG operated in compliance with the requirements and general advice on technical requirements and accreditation of bodies for anyone who is to check, test and certify gaming activities. This included tests for probability (to ensure the expected number of occurrences), randomness (so that one cannot predict the following occurrence with any degree of certainty) and uniformity (to determine that each possible outcome is equally likely over the long-term). The acceptance criteria for the statistical tests are a pass at a 95% confidence level.

1. OUTPUT BASED TESTING ON SCALED RANGES: 0-33, 0-36, 0-51, 0-66, 0-99, 0-500, 0-999

a. OUTPUT BASED TESTING ON SCALED RANGES RESULTS

OUTPUT BASED TESTING				CLIENT GENERATED DATA			eCOGRA GENERATED DATA		
Test Number	Sample Size	Test Range	DoF	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value
1	3 000 000	0-33	33	0.0546	0.1654	0.7409	0.4490	0.1662	0.9031
2	3 000 000	0-36	36	0.5787	0.1351	0.6130	0.3407	0.6739	0.2791
3	3 000 000	0-51	51	0.3715	0.2239	0.9788	0.7205	0.2494	0.4805
4	3 000 000	0-66	66	0.3747	0.5126	0.3334	0.2410	0.3226	0.3795
5	3 000 000	0-99	99	0.1335	0.6171	0.1638	0.4287	0.2507	0.4434
6	3 000 000	0-500	500	0.1749	0.1282	0.1407	0.6908	0.9266	0.0486
7	3 000 000	0-999	999	0.1120	0.5871	0.7999	0.6717	0.3595	0.9497

b. SCALED DATA RANDOMNESS TEST SUCCESS (✓) OR FAILURE (×) SUMMARY

OUTPUT BASED TESTING				CLIENT GENERATED DATA			eCOGRA GENERATED DATA		
Test Number	Sample Size	Test Range	DoF	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value
1	3 000 000	0-33	33	✓	✓	✓	✓	✓	✓
2	3 000 000	0-36	36	✓	✓	✓	✓	✓	✓
3	3 000 000	0-51	51	✓	✓	✓	✓	✓	✓
4	3 000 000	0-66	66	✓	✓	✓	✓	✓	✓
5	3 000 000	0-99	99	✓	✓	✓	✓	✓	✓
6	3 000 000	0-500	500	✓	✓	✓	✓	✓	✓
7	3 000 000	0-999	999	✓	✓	✓	✓	✓	✓

2. OUTPUT BASED TESTING ON SHUFFLED DECKS

a. OUTPUT BASED TESTING ON SHUFFLED DECKS RESULTS

OUTPUT BASED TESTING				CLIENT GENERATED DATA			eCOGRA GENERATED DATA		
Test Number	Sample Size	Test Range	DoF	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value
1	3 000 000	5 Card Hands	8	0.1654	0.2791	0.3847	0.6283	0.5570	0.5016
2	3 000 000	7 Card Hands	9	0.2810	0.0830	0.6553	0.4260	0.7149	0.4520
3	3 000 000	5-7 Card Multiples Combinations	17	0.4473	0.4735	0.5019	0.4112	0.5958	0.3327
4	3 000 000	5-7 Card Suit Combinations	29	0.3189	0.4398	0.3585	0.5666	0.3377	0.6979

b. SHUFFLED DECKS RANDOMNESS TEST SUCCESS (✓) OR FAILURE (×) SUMMARY

OUTPUT BASED TESTING				CLIENT GENERATED DATA			eCOGRA GENERATED DATA		
Test Number	Sample Size	Test Range	DoF	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value	Sample 1 P-value	Sample 2 P-value	Sample 3 P-value
1	3 000 000	5 Card Hands	8	✓	✓	✓	✓	✓	✓
2	3 000 000	7 Card Hands	9	✓	✓	✓	✓	✓	✓
3	3 000 000	5-7 Card Multiples Combinations	17	✓	✓	✓	✓	✓	✓
4	3 000 000	5-7 Card Suit Combinations	29	✓	✓	✓	✓	✓	✓

3. DIEHARD TESTS

a. DIEHARD TEST RESULTS

DIEHARD TEST		CLIENT GENERATED DATA			eCOGRA GENERATED DATA		
Test Name	Sample Size	Sample 1	Sample 2	Sample 3	Sample 1	Sample 2	Sample 3
BIRTHDAY SPACINGS TEST	48 000 000	0.2399	0.0958	0.0167	0.0249	0.0335	0.3579
OVERLAPPING 5-PERMUTATION TEST	48 000 000	0.1917	0.7044	0.0434	0.4604	0.5267	0.2769
THE BITSTREAM TEST	48 000 000	0.0404	0.0243	0.0733	0.0570	0.0682	0.0736
COUNT-THE-1's TEST bytes	48 000 000	0.0135	0.0102	0.0016	0.0617	0.0025	0.0403
MINIMUM DISTANCE TEST	48 000 000	0.6828	0.9373	0.4734	0.3491	0.2754	0.6841
SQUEEZE TEST	48 000 000	0.4051	0.4440	0.9087	0.5923	0.1672	0.5751
RUNS TEST	48 000 000	0.4160	0.0774	0.2863	0.3408	0.1754	0.2532
CRAPS TEST	48 000 000	0.0199	0.2318	0.3086	0.8674	0.8225	0.4684

b. DIEHARD TESTS SUCCESS (✓) OR FAILURE (✗) SUMMARY

DIEHARD TEST		CLIENT GENERATED DATA			eCOGRA GENERATED DATA		
Test Name	Sample Size	Sample 1	Sample 2	Sample 3	Sample 1	Sample 2	Sample 3
BIRTHDAY SPACINGS TEST	48 000 000	✓	✓	✓	✓	✓	✓
OVERLAPPING 5-PERMUTATION TEST	48 000 000	✓	✓	✓	✓	✓	✓
THE BITSTREAM TEST	48 000 000	✓	✓	✓	✓	✓	✓
COUNT-THE-1's TEST bytes	48 000 000	✓	✓	✓	✓	✓	✓
MINIMUM DISTANCE TEST	48 000 000	✓	✓	✓	✓	✓	✓
SQUEEZE TEST	48 000 000	✓	✓	✓	✓	✓	✓
RUNS TEST	48 000 000	✓	✓	✓	✓	✓	✓
CRAPS TEST	48 000 000	✓	✓	✓	✓	✓	✓

4. SERIAL CORRELATION TESTS

a. SERIAL CORRELATION TEST RESULTS:

	CLIENT GENERATED DATA					ECOGRA GENERATED DATA				
	DECK 1					DECK 1				
	Col 1	Col 2	Col 3	Col 4	Col 5	Col 1	Col 2	Col 3	Col 4	Col 5
LAG 1	0.7029	0.2453	0.4932	0.1460	0.4726	0.5814	0.3263	0.5467	0.0313	0.4281
LAG 2	0.2417	0.3268	0.1660	0.3472	0.3126	0.4499	0.5968	0.8328	0.0925	0.6924
LAG 3	0.3361	0.5082	0.2387	0.5121	0.4494	0.5570	0.1935	0.9464	0.1678	0.3920
LAG 4	0.4781	0.4689	0.2241	0.6350	0.4414	0.6301	0.2703	0.9641	0.2506	0.1694
LAG 5	0.5050	0.6114	0.1319	0.6145	0.3888	0.5638	0.3468	0.9413	0.3527	0.1841
LAG 6	0.4504	0.6865	0.2010	0.7354	0.1807	0.6622	0.3477	0.9539	0.4436	0.1515
LAG 7	0.5270	0.7677	0.2871	0.7496	0.2611	0.5502	0.2789	0.8805	0.5164	0.1613
LAG 8	0.3992	0.4876	0.2469	0.8305	0.3371	0.0900	0.3720	0.4444	0.5377	0.1755
LAG 9	0.4810	0.4097	0.0406	0.8757	0.4316	0.1330	0.3315	0.3598	0.5197	0.2387
LAG 10	0.5478	0.3554	0.0421	0.9083	0.5206	0.1866	0.4079	0.2765	0.4514	0.3028

b. SERIAL CORRELATION TEST SUCCESS (✓) OR FAILURE (×) SUMMARY

	CLIENT GENERATED DATA					ECOGRA GENERATED DATA				
	DECK 1					DECK 1				
	Col 1	Col 2	Col 3	Col 4	Col 5	Col 1	Col 2	Col 3	Col 4	Col 5
LAG 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

5. CORRELATION TESTS

a. CORRELATION TEST RESULTS:

	CLIENT GENERATED DATA							eCOGRA GENERATED DATA						
Range	0-33	0-36	0-51	0-66	0-99	0-500	0-999	0-33	0-36	0-51	0-66	0-99	0-500	0-999
LAG 1	0.7436	0.0499	0.6740	0.5370	0.6022	0.5950	0.2155	0.5360	0.5805	0.4934	0.2412	0.8720	0.7046	0.4467
LAG 2	0.6885	0.1463	0.4678	0.5875	0.7190	0.1983	0.2652	0.7400	0.7099	0.4022	0.4161	0.0504	0.7635	0.7485
LAG 3	0.5871	0.2075	0.5410	0.7611	0.3752	0.1711	0.3237	0.8495	0.7533	0.5502	0.5422	0.0226	0.9093	0.8346
LAG 4	0.6993	0.3358	0.7037	0.3443	0.4545	0.2489	0.4329	0.8323	0.7612	0.7136	0.7081	0.0175	0.6835	0.9296
LAG 5	0.7497	0.2752	0.8091	0.4012	0.5640	0.3689	0.5660	0.9026	0.8576	0.6384	0.7814	0.0275	0.6830	0.9070
LAG 6	0.8279	0.3714	0.3600	0.5220	0.6867	0.4911	0.6754	0.9230	0.9212	0.7009	0.8355	0.0126	0.6705	0.8949
LAG 7	0.8610	0.4048	0.4274	0.6378	0.7827	0.6067	0.7495	0.9440	0.9201	0.6201	0.8786	0.0190	0.7590	0.9241
LAG 8	0.9109	0.5103	0.3356	0.7269	0.8591	0.5399	0.8330	0.9441	0.9573	0.7221	0.8158	0.0299	0.7220	0.8252
LAG 9	0.6862	0.6097	0.4195	0.7576	0.8991	0.6301	0.8593	0.9673	0.8446	0.6318	0.8800	0.0449	0.7072	0.8727
LAG 10	0.6106	0.3984	0.3662	0.8232	0.5896	0.5286	0.9069	0.8530	0.4790	0.6434	0.8281	0.0674	0.7840	0.8474

b. CORRELATION TEST SUCCESS (✓) OR FAILURE (✗) SUMMARY

	CLIENT GENERATED DATA							eCOGRA GENERATED DATA						
Range	0-33	0-36	0-51	0-66	0-99	0-500	0-999	0-33	0-36	0-51	0-66	0-99	0-500	0-999
LAG 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LAG 10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓