Test report - Megapot V2 RNG

Product Data	
Product name:	Megapot V2 RNG
Product type:	Random Number Generator
Version:	1.0

Applicant Data	
Applicant:	MEGAPOT INC
Applicant Address:	Megapot Inc c/o BZAGENTS Limited 24 San Victor St
Applicant Contact:	Michael Boremi
Manufacturer name:	MEGAPOT INC
Manufacturer address:	Megapot Inc c/o BZAGENTS Limited 24 San Victor St Orange Walk Town, Orange Walk Belize

DISCLAIMER

Copyright © Lean Lab Company Limited, Malta. All rights reserved. This test report may not be reproduced, other than in full, except with the prior written permission of the issuing Accredited Testing Facility. Application of the copyright notice and disclaimer is obligatory. Lean Lab Company Limited disclaims liability for any direct, indirect, consequential or incidental damages that may result from the use of the information or data, or from the inability to use the information or data.
The results included in this report are based on the data as provided by the client.

Report ID: CHERRY.199926.MGA.R0
Report filename: CHERRY.199926.MGA.R0_MegapotV2RNG_MEGAPOTINC
Product name: Megapot V2 RNG
Test house: Lean Lab Company Limited (MO.2, Ruby Ninu, Pendergardens, Block 17, Level 1, Triq Gort, San Giljan, STJ 9023, Malta)
Compliance Verdict: Compliant

Report Data	
Report Issue Date:	07/08/2026
References:	https://docs.pyth.network/entropy; https://en.wikipedia.org/wiki/Fisher%E2%80%93Yates_shuffle; https://en.wikipedia.org/wiki/Rejection_sampling;
Platform and version:	N/A (RNG report only)
Test House:	Lean Lab Company Limited
Test House Address:	MO.2, Ruby Ninu, Pendergardens, Block 17, Level 1, Triq Gort, San Giljan, STJ 9023, Malta
Project Engineer(s) (incl. ext. providers):	Todor Balabanov
Quality Manager:	Ventsislav Kirchev
Peer Review:	Neven Panchev
Project Coordination:	Ivaylo Georgiev
Technical Responsible Person:	Mihael Mladenov
Source Code Receipt Date:	22/01/2026
Test Period:	25/01/2026 - 05/02/2026
Jurisdiction:	Malta

Report ID: CHERRY.199926.MGA.R0
Report filename: CHERRY.199926.MGA.R0_MegapotV2RNG_MEGAPOTINC
Product name: Megapot V2 RNG
Test house: Lean Lab Company Limited (MO.2, Ruby Ninu, Pendergardens, Block 17, Level 1, Triq Gort, San Giljan, STJ 9023, Malta)
Compliance Verdict: Compliant

Table Of Contents

ABOUT THE TEST HOUSE
PREFACE
METHODOLOGY
ASSESSMENT SCOPE
TEST EQUIPMENT
IN-HOUSE TOOLS
SAMPLING
REQUIREMENTS
SOFTWARE IDENTIFICATION
TEST RESULTS
STATISTICAL ANALYSIS
SOURCE CODE ASSESSMENT
CONCLUSION

ABOUT THE TEST HOUSE

Lean Lab Company Limited (hereinafter known as “RiskCherry”) provides compliance assessment services to the gaming industry and authorities. The laboratory is stationed in MO.2, Ruby Ninu, Pendergardens, Block 17, Level 1, Triq Gort, San Giljan, STJ 9023, Malta. All testing activities are carried out at the location Georgi S. Rakovski Street 128, 4th floor, Sofia Bulgaria. In certain cases the client’s facility would also be used at its specified location. RiskCherry has obtained the relevant accreditation related to testing and assessment of random number generators.

RiskCherry implements cutting edge technology and process management to provide leaders in the industry with high quality assessment in a short period of time. Every report issued under the RiskCherry logo undergoes rigorous checks and automatic validations before reaching our clients.

PREFACE

This report represents the identification of the gaming product under assessment, information about the laboratory, scope and methodology used, the applied scope of assessment, a list of all executed tests associated directly with the assessment scope, and RiskCherry’s final verdict of compliance with regards to the tested product. The report has been issued under the supervision of RiskCherry’s assigned Quality Manager, or the Head of Compliance and Quality. The accuracy and truthfulness of this report have been fully assessed during a strict mandatory quality assessment. If report errors are detected, the client should contact their assigned customer service representative.

RiskCherry reserves the right to issue report revisions in such cases when additional information relevant to the validity of the report has presented itself to the test laboratory. In case an amendment to the report is required, a new report is issued with an incremented Revision index (R0) to the Report ID, and the Revision Info section is filled in detailing the reasons for the new Revision while making a direct reference to the old Revision via Report ID.

METHODOLOGY

RiskCherry provides assessment of gaming systems using officially recognized and accredited assessment methods. These methods cover all applicable components of the product in scope. Our test engineers carry out testing by applying elaborate techniques such as documentation evaluation, source code analysis, statistical assessment of simulations, functional tests and visual assessment to ensure the product complies with all relevant requirements.

All testing activities are performed under strict supervision of Head of Compliance & Quality and the Technical Director in a controlled and isolated environment. In cases where external parties or factors have had influence on the testing, this shall be explicitly stated in this document. In cases where sampling is performed as part of the test procedure, this shall be explicitly stated in the document. The document shall include a detailed account of any samples taken, including but not limited to: the date of sampling, sampling method performed, sampling location and any other internal or external factors which may have had an impact on the sampling. Any other deviations from the methodology stated in this section shall be explicitly stated in this document. The specific scope of methods used in this test report are referenced in the Assessment Scope section. If individual opinions/interpretations with regards to the achieved test results need to be included in the report, the report explicitly states the basis for their inclusion, the name and qualifications of the personnel authorized to express them. When opinions/interpretations are directly communicated by dialogue with the applicant, a record of the dialogue is retained. All opinion/interpretation expressions are approved by the Quality Manager, or the Head of Compliance and Quality.

ASSESSMENT SCOPE

The applicant has requested from the laboratory to assess the product as provided by the applicant in its entirety against all relevant official requirement, as listed below. Only requirements related to random number generators have been tested. All requirements related to supplier and operator game, platform, security, system changes and any other non-RNG elements fall out of scope for this report.

- Remote gambling and software technical standards February 2021 (updated with 17 January 2025 changes)

TEST EQUIPMENT

During RNG assessment, RiskCherry always uses the latest stable version of the applicable test suites and tools.

Device	Operating System	R Stats Tool	Dieharder Test Suite	NIST Test Suite	Kolmogorov-Smirnov Test Suite
HP ProBook 450	Windows 11 Pro	4.5.2 for Windows	3.31.1	DAVE 2.5	4.6.0

IN-HOUSE TOOLS

Name	Version	Description
cherry-doc-generator	2.1	Generates reports based on pre-defined templates per jurisdiction.

SAMPLING

The statistical analysis testing of the RNG is performed using a binary data file which contains an array of at least 10GB randomly generated 32-bit little endian unsigned integers using the RNG submitted for testing. The sample is generated on a system which is set up and configured as close as possible to the production environment where the RNG will be used live.

ID	Sampling Date	Sample Size	Sampling Method	Sampling Location	Sampling Population
coordinationlabs_order-CLA-11_Megapot_raw_entropy_bin	2026-01-26	10GB	Simple Random Sampling	San Francisco, CA, USA	Random number generator

REQUIREMENTS

Verdict	Requirement Ref.	Requirement Text (English)
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	1A	Where customers hold a credit or debit balance, the pages or screens used for gambling and to move money into and out of accounts must display the customer's current account balance, in the currency of their account (eg dollars, euros or pounds sterling), whenever that customer is logged in. Where it is not practical to display current balance from gambling screens then easily accessible links to this information must be provided.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	1B	Customers must have easy access to at least three months account and gambling history without having to contact the licensee. A minimum of 12 months of gambling and account history must be made available on request. The ability to request this information should be made clear to customers and be provided as soon as is practicable.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	1C	Customers must be able to access information about their net deposits.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	2A	The remote gambling system must make available clear information about the amount of money being gambled by the customer, including any conversions from one form of currency to another, or from currency to credits, chips or other tokens etc, at the point of conversion.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	2B	The gambling system must display sufficient relevant information about the customer's gamble so that the content of the gamble is clear. This information must be made available before the customer commits to the gamble including, for example, in the artwork and textual information displayed during gaming, or on an electronic equivalent of a betting slip or lottery ticket.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	2C	The gambling system must enable customers to choose whether to accept price fluctuations (in either direction) that occur after their bet is requested.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	2D	Customers who choose to use third party user interfaces must be informed that applications may not display full information about their gambles.
N/A (This requirement is not applicable for MGA)	2E	All gaming sessions must clearly display a customer's net position, in the currency of their account or product (e.g. pounds sterling, dollar, Euro) since the session started.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	3A	An explanation of the applicable rules must be easily available to the customer before they commit to gamble. The content including artwork and text must be accurate, and sufficient to explain all of the applicable rules and how to participate. All reasonable steps must be taken to ensure that the content is understandable.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	3A-JP	An explanation of the applicable rules must be easily available to the customer before they commit to gamble. The content including artwork and text must be accurate, and sufficient to explain all of the applicable rules and how to participate. All reasonable steps must be taken to ensure that the content is understandable.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	3B	Where relevant, as the game or event progresses, information that may reasonably be expected to enable the customer to understand the current state must be displayed.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	3C	For each virtual event, game (including bingo), or lottery, information that may reasonably be expected to enable the customer to make an informed decision about his or her chances of winning must be easily available before the customer commits to gamble. Information must include: i. a description of the way the game works and the way in which winners are determined and prizes allocated ii. house edge (or margin) iii. the return to player (RTP) percentage or iv. the probability (likelihood) of winning events occurring.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	3D	For each virtual event, game (including bingo), or lottery, content describing the potential prizes and payouts or the means by which these are calculated or determined must be easily available before the customer commits to gamble.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	3D-JP	For each virtual event, game (including bingo), or lottery, content describing the potential prizes and payouts or the means by which these are calculated or determined must be easily available before the customer commits to gamble.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	4A	Where speed of interaction has a significant effect on the customer's chance of winning, operators must assess the level of risk and demonstrate to the Commission that they are taking reasonable steps to reduce the risk to customers.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	4B	For time-critical events, the customer should be informed that they might be at a disadvantage because of technical issues such as slower network speeds, or slower end user device performance.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	5A-1	All reasonable steps should be taken to ensure that gambles are accepted, processed and settled in accordance with the operators' published terms and rules, and the rules of the specific game, event, or bet.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	5A-2	Where unexpected system flaws, faults, or errors that affect the customer occur, steps are to be taken as soon as practicable to remedy the problem and ensure that the customer is treated fairly according to the circumstances.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	6A	Play-for-free games must implement the same game rules as the corresponding play-for-money games offered on the same facilities (ie the same website). Operators must take all reasonable steps to ensure that play-for-free games accurately represent the likelihood of winning and prize distribution in the play-for-money game. For the purpose of this requirement playing a game includes participating in a lottery and/or betting on a virtual event.
Compliant	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 (ie a compensated game) is not permitted. Where lotteries use the outcome of other events external to the lottery, to determine the result of the lottery the outcome must be unpredictable and externally verifiable.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	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.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	7C	Game designs or features that may reasonably be expected to mislead the customer about the likelihood of particular results occurring are not permitted, including substituting losing events with near-miss losing events and simulations of real devices that do not simulate the real probabilities of the device.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	7C-JP	Game designs or features that may reasonably be expected to mislead the customer about the likelihood of particular results occurring are not permitted, including substituting losing events with near-miss losing events and simulations of real devices that do not simulate the real probabilities of the device.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	7D	The rules, payouts and outcome probabilities of a virtual event or game may not be changed while it is available for gambling, except as provided for in the rules of the game, lottery or virtual event. Such changes must be brought to customer's attention.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	7E	Except in the case of subscription lotteries, the system clearly and accurately display the result of the game or event and the customer's gamble. The result must be displayed for a length of time that may reasonably be expected to be sufficient for the customer to understand the result of the game or event in the context of their gamble.
N/A (This requirement is not applicable for MGA)	8A	The gambling system must require a customer to commit to each game cycle individually.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	9A	An explanation of the jackpot rules must be clearly available to the customer before they commit to gamble.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	9B	Jackpot systems must be configured and operated with adequate fairness and security.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	10A	Operators must take all reasonable steps to ensure that their policies for instigating or dealing with service interruptions are fair and do not systematically disadvantage customers.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	10B	Systems must be capable of recovering from failures that cause interruptions to gambling, including where appropriate, the capability to void gambles (with or without manual intervention), the capability to suspend betting markets, and taking all reasonable steps to retain sufficient information to be able to restore events to their pre-failure state.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	10C	Operators must make available information about their policies regarding service interruptions in various different circumstances.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	11A	Measures intended to deter, prevent, and detect collusion and cheating must be implemented. Gambling systems must retain a record of relevant activities to facilitate investigation and be capable of suspending or disabling player accounts or player sessions. Operators must monitor the effectiveness of their policies and procedures.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	11B	Information must be made available about the operator's policies and procedures with regard to cheating, recovered player funds and about how to complain if a customer suspects other participants are cheating.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	12A	The gambling system must provide easily accessible facilities for customers to set their own financial limits at any time from the point of registration. Customers must be prompted to set a limit as part of the registration process or at the point at which the customer makes the first deposit or payment. The limit must be implemented as soon as practicable after the customer's request. The customer must be informed when the limit will come into force.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	12B	Customers must be presented with a 'free text' box to set a limit, or the equivalent in the case of telephone gambling. As a minimum, limits must be applied at the account level.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	12C	Financial limit facilities must be provided via a direct link on the homepage and be clearly visible and accessible. Financial limit facilities must be clearly visible and accessible on deposit pages/screens or via a direct link on these pages or screens. The gambling system must minimise the number of clicks or pages customers make in order to access financial limit facilities.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	12D	Customer-led limits must only be increased at the customer's request, only after a cooling-off period of at least 24 hours has elapsed and only once the customer has taken positive action at the end of the cooling off period to confirm their request. Unless systems/technical failures prevent it, customer-led reductions to limits must be implemented immediately. The gambling system must provide a prompt to customers to review their own account and transaction information, as is currently made available under RTS 1 – Customer account information. This must be provided at a minimum of six-month intervals for accounts with activity within a rolling 12-month period. Customers must be provided with facilities to set more frequent reminders to receive this statement and review their limits.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	12E	Financial limit-setting facilities must present setting a limit as the default choice. The gambling system must require an action by the customer in order to decline setting a limit. The gambling system must receive confirmation that the customer does not wish to set a limit before moving on to deposit/gamble. The gambling system must prompt existing customers without limits set to review this position as a minimum on an annual basis.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	13A	Where the gambling system uses full screen client applications that obscure the clock on the customer's device the client application itself must display the time of day or the elapsed time since the application was started, wherever practicable.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	13B	The gambling system must provide easily accessible facilities that make it possible for customers to set a frequency at which they will receive and see on the screen a reality check within a gaming session. A 'reality check' means a display of the time elapsed since the session began. The customer must acknowledge the reality check for it to be removed from the screen.
N/A (This requirement is not applicable for MGA)	13C	The elapsed time should be displayed for the duration of the gaming session.
N/A (This requirement is not applicable for MGA)	14A	Gambling products must not actively encourage customers to chase their losses, increase their stake or increase the amount they have decided to gamble, or continue to gamble after they have indicated that they wish to stop.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	14B	Consumers must not be given the option to cancel their withdrawal request.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	14C	The gambling system must not offer functionality which facilitates playing multiple games at the same time.

N/A (This requirement is not applicable for MGA)	14D	It must be a minimum of 2.5 seconds from the time a game is started until the next game cycle can be commenced. It must always be necessary to release and then depress the 'start button' or take equivalent action to commence a game cycle.
N/A (This requirement is not applicable for MGA)	14E	The gambling system must not permit a customer to reduce the time until the result is presented.
N/A (This requirement is not applicable for MGA)	14F	The gambling system must not celebrate a return which is less than or equal to the total stake gambled.
N/A (This requirement is not applicable for MGA)	14G	It must be a minimum of 5 seconds from the time a game is started until the next game cycle can be commenced. It must always be necessary to release and then depress the 'start button' or take equivalent action to commence a game cycle.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	15A	Information must be made available that explains that 'live' TV or other broadcasts are delayed and that others may have more up-to-date information. Main in-play betting pages must include this information where practicable.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	16A	Where peer-to-peer customers may be gambling against programs deployed by other customers to play on their behalf, or customers assisted by third party software, information should be made available that describes that this is possible, and if it is against the operator's terms and conditions, how to report suspected use.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	16B	Operators must make it clear to players whether the use of third party software is permitted and if so which types. Operators that prohibit certain types of third party software must implement measures intended to deter, prevent, and detect their use.

N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	16C	Where operators use programs to participate in gambling on their behalf in peer-to-peer gambling, easily accessible information must be displayed, which clearly informs customers that the operator uses this kind of software.
N/A (This requirement is not related to random number generator assessment and it falls out of scope.)	17A	Live dealer operations must be fair and independently auditable.

SOFTWARE IDENTIFICATION

Software identification has been achieved using the "sha1sum" program and the SHA-1 algorithm.

File	Version	Hash
Entropy.sol	2.2.1	068da6a5a53e538123c9b8f4499b1289902d2ac1
ScaledEntropyProvider.sol	1.0.0	28f2df4ad75620ba3f8b92a8578b6a07b59c71e7
FisherYatesWithRejection.sol	1.0.0	0b425843094089050a2aeefd7382dc8ef163079b
IScaledEntropyProvider.sol	1.0.0	0aa8fef14e60c80df29a93bb25abeacca47f5411
state.rs	9.4.0	7198f57148916f565454194510caee3e68cb9237

TEST RESULTS

Kolmogorov-Smirnov Test (R)

Test: One-sample KS test

D statistic: 1.5e-05 (minimal difference from expected distribution)

p-value: 1

Interpretation:

The data distribution matches the expected uniform distribution extremely well. A p-value of 1 suggests there is no significant deviation from randomness according to this test.

DieHarder Test Suite Results

Most tests PASSED, meaning the data appears random under these metrics.

WEAK results:

Test: rgb_lagged_sum

p-value: 0.00245689

Test: rgb_kstest_test

p-value: 0.99733749

Interpretation:

A WEAK result isn't a failure but suggests the result is close to an edge case (very high or very low p-value). Typically, p-values near 0 or 1 raise caution, though WEAKs in an oversized suite isn't unusual.

Summary:

The data appear highly random, as indicated by both the KS test and the Dieharder battery.

For general randomness requirements, they are solid.

```
binary_data <- readBin("coordinationlabs_order-CLA-11_Megapot_raw_entropy_bin", what = "integer", n =
100000, size = 4, endian = "little")
ordered_values <- rank(binary_data) / length(binary_data)
expected_uniform <- seq(0, 1, length.out = length(binary_data))
ks_result <- ks.test(ordered_values, "punif", 0, 1)
print(ks_result)

      One-sample Kolmogorov-Smirnov test
data:  ordered_values
D = 1.5e-05, p-value = 1
alternative hypothesis: two-sided



dieharder -a -g 201 -f coordinationlabs_order-CLA-11_Megapot_raw_entropy_bin

#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|coordinationlabs_order-CLA-11_Megapot_raw_entropy_bin|  1.57e+07  |
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
```

Report ID: CHERRY.199926.MGA.R0
Report filename: CHERRY.199926.MGA.R0_MegapotV2RNG_MEGAPOTINC
Product name: Megapot V2 RNG
Test house: Lean Lab Company Limited (MO.2, Ruby Ninu, Pendergardens, Block 17, Level 1, Triq Gort, San Giljan, STJ 9023, Malta)
Compliance Verdict: Compliant

diehard_birthdays	0	100	100	0.30267656	PASSED
diehard_operm5	0	1000000	100	0.70405132	PASSED
diehard_rank_32x32	0	40000	100	0.09522210	PASSED
diehard_rank_6x8	0	100000	100	0.13425971	PASSED
diehard_bitstream	0	2097152	100	0.83726471	PASSED
diehard_opso	0	2097152	100	0.81403688	PASSED
diehard_oqso	0	2097152	100	0.63857632	PASSED
diehard_dna	0	2097152	100	0.69707768	PASSED
diehard_count_1s_str	0	256000	100	0.81371377	PASSED
diehard_count_1s_byt	0	256000	100	0.21681839	PASSED
diehard_parking_lot	0	12000	100	0.54496665	PASSED
diehard_2dsphere	2	8000	100	0.17784069	PASSED
diehard_3dsphere	3	4000	100	0.45599287	PASSED
diehard_squeeze	0	100000	100	0.34549938	PASSED
diehard_sums	0	100	100	0.02171337	PASSED
diehard_runs	0	100000	100	0.69812256	PASSED
diehard_runs	0	100000	100	0.70096518	PASSED
diehard_craps	0	200000	100	0.05181271	PASSED
diehard_craps	0	200000	100	0.70270760	PASSED
marsaglia_tsang_gcd	0	10000000	100	0.51878576	PASSED
marsaglia_tsang_gcd	0	10000000	100	0.83831869	PASSED
sts_monobit	1	100000	100	0.19171684	PASSED
sts_runs	2	100000	100	0.97524304	PASSED
sts_serial	1	100000	100	0.85310917	PASSED
sts_serial	2	100000	100	0.69113036	PASSED
sts_serial	3	100000	100	0.97440788	PASSED
sts_serial	3	100000	100	0.64816776	PASSED
sts_serial	4	100000	100	0.59571734	PASSED
sts_serial	4	100000	100	0.05418906	PASSED
sts_serial	5	100000	100	0.61535896	PASSED
sts_serial	5	100000	100	0.49126998	PASSED
sts_serial	6	100000	100	0.60454377	PASSED
sts_serial	6	100000	100	0.49113781	PASSED
sts_serial	7	100000	100	0.32374536	PASSED
sts_serial	7	100000	100	0.47589458	PASSED
sts_serial	8	100000	100	0.31291175	PASSED
sts_serial	8	100000	100	0.36709276	PASSED
sts_serial	9	100000	100	0.39161507	PASSED
sts_serial	9	100000	100	0.24135203	PASSED
sts_serial	10	100000	100	0.38759414	PASSED
sts_serial	10	100000	100	0.84045001	PASSED
sts_serial	11	100000	100	0.97940618	PASSED
sts_serial	11	100000	100	0.61926916	PASSED
sts_serial	12	100000	100	0.91721592	PASSED
sts_serial	12	100000	100	0.76086526	PASSED
sts_serial	13	100000	100	0.97891311	PASSED
sts_serial	13	100000	100	0.81895854	PASSED
sts_serial	14	100000	100	0.89109717	PASSED
sts_serial	14	100000	100	0.35434423	PASSED
sts_serial	15	100000	100	0.96935466	PASSED
sts_serial	15	100000	100	0.23017843	PASSED
sts_serial	16	100000	100	0.45323615	PASSED
sts_serial	16	100000	100	0.65759710	PASSED
rgb_bitdist	1	100000	100	0.12301255	PASSED
rgb_bitdist	2	100000	100	0.83784988	PASSED
rgb_bitdist	3	100000	100	0.97602306	PASSED
rgb_bitdist	4	100000	100	0.49398025	PASSED
rgb_bitdist	5	100000	100	0.30938234	PASSED
rgb_bitdist	6	100000	100	0.65322162	PASSED
rgb_bitdist	7	100000	100	0.97529532	PASSED
rgb_bitdist	8	100000	100	0.45651601	PASSED
rgb_bitdist	9	100000	100	0.36641931	PASSED
rgb_bitdist	10	100000	100	0.02858235	PASSED

Report ID: CHERRY.199926.MGA.R0
Report filename: CHERRY.199926.MGA.R0_MegapotV2RNG_MEGAPOTINC
Product name: Megapot V2 RNG
Test house: Lean Lab Company Limited (MO.2, Ruby Ninu, Pendergardens, Block 17, Level 1, Triq Gort, San Giljan, STJ 9023, Malta)
Compliance Verdict: Compliant

```
          rgb_bitdist|  11|    100000|     100|0.48649001|  PASSED
          rgb_bitdist|  12|    100000|     100|0.36223486|  PASSED
rgb_minimum_distance|   2|     10000|    1000|0.48846450|  PASSED
rgb_minimum_distance|   3|     10000|    1000|0.98749083|  PASSED
rgb_minimum_distance|   4|     10000|    1000|0.13524242|  PASSED
rgb_minimum_distance|   5|     10000|    1000|0.53190095|  PASSED
    rgb_permutations|   2|    100000|     100|0.89680878|  PASSED
    rgb_permutations|   3|    100000|     100|0.23293628|  PASSED
    rgb_permutations|   4|    100000|     100|0.95546324|  PASSED
    rgb_permutations|   5|    100000|     100|0.75648135|  PASSED
      rgb_lagged_sum|   0|   1000000|     100|0.64779678|  PASSED
      rgb_lagged_sum|   1|   1000000|     100|0.86397554|  PASSED
      rgb_lagged_sum|   2|   1000000|     100|0.37488895|  PASSED
      rgb_lagged_sum|   3|   1000000|     100|0.24924608|  PASSED
      rgb_lagged_sum|   4|   1000000|     100|0.85304140|  PASSED
      rgb_lagged_sum|   5|   1000000|     100|0.07919709|  PASSED
      rgb_lagged_sum|   6|   1000000|     100|0.21976975|  PASSED
      rgb_lagged_sum|   7|   1000000|     100|0.86461981|  PASSED
      rgb_lagged_sum|   8|   1000000|     100|0.23705250|  PASSED
      rgb_lagged_sum|   9|   1000000|     100|0.97482330|  PASSED
     rgb_lagged_sum|  10|   1000000|     100|0.70180425|  PASSED
     rgb_lagged_sum|  11|   1000000|     100|0.05126521|  PASSED
     rgb_lagged_sum|  12|   1000000|     100|0.69835104|  PASSED
     rgb_lagged_sum|  13|   1000000|     100|0.27359223|  PASSED
     rgb_lagged_sum|  14|   1000000|     100|0.80787356|  PASSED
     rgb_lagged_sum|  15|   1000000|     100|0.11292279|  PASSED
     rgb_lagged_sum|  16|   1000000|     100|0.99281069|  PASSED
     rgb_lagged_sum|  17|   1000000|     100|0.86472021|  PASSED
     rgb_lagged_sum|  18|   1000000|     100|0.44507636|  PASSED
     rgb_lagged_sum|  19|   1000000|     100|0.78869370|  PASSED
     rgb_lagged_sum|  20|   1000000|     100|0.89227058|  PASSED
     rgb_lagged_sum|  21|   1000000|     100|0.46479294|  PASSED
     rgb_lagged_sum|  22|   1000000|     100|0.20499021|  PASSED
     rgb_lagged_sum|  23|   1000000|     100|0.06134879|  PASSED
     rgb_lagged_sum|  24|   1000000|     100|0.80184757|  PASSED
     rgb_lagged_sum|  25|   1000000|     100|0.13132749|  PASSED
     rgb_lagged_sum|  26|   1000000|     100|0.93098563|  PASSED
     rgb_lagged_sum|  27|   1000000|     100|0.87640953|  PASSED
     rgb_lagged_sum|  28|   1000000|     100|0.88946841|  PASSED
     rgb_lagged_sum|  29|   1000000|     100|0.91957133|  PASSED
     rgb_lagged_sum|  30|   1000000|     100|0.49171155|  PASSED
     rgb_lagged_sum|  31|   1000000|     100|0.00245689|   WEAK
     rgb_lagged_sum|  32|   1000000|     100|0.16016828|  PASSED
   rgb_kstest_test|   0|     10000|    1000|0.99733749|   WEAK
   dab_bytedistrib|   0|  51200000|       1|0.09099602|  PASSED
           dab_dct| 256|     50000|       1|0.94098248|  PASSED
      dab_filltree|  32|  15000000|       1|0.74369801|  PASSED
      dab_filltree|  32|  15000000|       1|0.25568298|  PASSED
     dab_filltree2|   0|   5000000|       1|0.23587584|  PASSED
     dab_filltree2|   1|   5000000|       1|0.23006633|  PASSED
      dab_monobit2|  12|  65000000|       1|0.93693331|  PASSED
```

STATISTICAL ANALYSIS

To ensure the generated pseudo-random numbers meet the criteria of being 'acceptably random,' the algorithm's output undergoes statistical analysis. This analysis involves a set of tests that assess the likelihood that the numbers were not produced by a process resembling true randomness. Each test examines a distinct aspect of the random number series, and failure occurs if the probability of a non-random process producing the series exceeds a predefined threshold. Among other verifications, these tests will determine whether the output from the RNG is uniformly distributed across the entire output range.

For statistical analysis of the output of the random number generator, a file was created containing 2.68 billion unsigned integer numbers (for a total of 10GB) generated by the RNG. For this generation, a test setup was used with an identical configuration as used in the production environment.

The main software used for statistical analysis of raw output is the Dieharder RNG test suite (Brown, 2015) or NIST test suite. Dieharder is a test suite maintained by Robert G. Brown from Duke University Physics Department. It builds upon the Diehard battery of tests from George Marsaglia (Marsaglia, 1995) but also includes tests from the statistical test suite from NIST (Soto, 1999) and tests developed by Robert G. Brown himself. Additionally, the statistical analysis incorporates the Kolmogorov-Smirnov test, which assesses the distributional similarity between the generated random numbers and an expected distribution, enhancing the robustness of the evaluation process.

The complete Dieharder suite was run using a sample of 2.68 billion random 32-bit unsigned integers (10 GB) generated with a platform similar to the production one. The test suite consists of independent tests. For each test, random numbers from the sample were used. Because the entire suite needs more than 10 billion random numbers, reuse of the random numbers from the data file was allowed, but not in the same test.

A detailed breakdown of the tests can be found in the section “Test Results”. All significant tests passed the first assessment.

SOURCE CODE ASSESSMENT

A source code assessment of the provided RNG has been conducted to ascertain all properties of the RNG required to fulfil the requirements defined in the assessment scope of this report. This list was identified to the best of RiskCherry's knowledge by analyzing the test item(s) and collecting all possible reputable information sources at the time of the testing activity.

Property	Assessment	Verdict
Source code language	Solidity, Rust	Compliant
OS/System Dependencies	Pyth Fortuna	Compliant
RNG implementation	The RNG uses the Pyth Entropy protocol (Fortuna) combined with a scaling layer to generate verifiably fair lottery numbers. Pyth Entropy (Fortuna) is a decentralized entropy provider that generates cryptographically secure random values using hash chains. How it works: 1. Provider pre-generates a hash chain from a secret seed 2. Hash chain values are revealed in sequence 3. Each revelation can be verified against the previous commitment 4. User cannot predict provider values; provider cannot predict user values Hash Chain Structure: seed → H(seed) → H(H(seed)) → H(H(H(seed))) → ...	Compliant
Source(s) of entropy	The system combines entropy from two independent sources using the Pyth Entropy protocol to produce verifiably fair lottery numbers. User and provider entropy are combined using: combined = keccak256(user_secret provider_revelation)</w:t><w:br/><w:t xml:space="preserve"></w:t><w:br/><w:t xml:space="preserve">This ensures: - Neither party can influence the output alone - The result is unpredictable until both values are revealed - The combination is deterministic and verifiable.	Compliant
Predictability of outputs	The RNG is unpredictable.	Compliant
Cycling and/or synchronization	Pyth Entropy Cycle The Pyth on-chain protocol’s logic: Commit phase: Provider posts a commitment to a random seed (x_i). User submission: User submits their own contribution (x_U). Reveal phase: Provider reveals the committed seed. Verification: The contract checks the hash chain correctness. Random output: Final randomness = hash(x_i, x_U). Callback: The resulting random number is sent to the requester via a callback.	Compliant
Security	Suitable for cryptographic secure purposes.	Compliant
Seeding	Seeding Initial seeding is the process of setting up the PRNG’s internal state using high-quality random bits. In Fortuna, this comes from the entropy pools or a seed file on disk. Reseeding Reseeding refreshes the generator’s internal state with new entropy collected since the last reseed. Why important? It ensures that even if the internal state is compromised at some point,	Compliant

	future outputs become unpredictable again once reseeded. Fortuna doesn't reseed on every entropy input — it uses the pool schedule (pool 0 every reseed, pool 1 every second, pool 2 every fourth, etc.) to ensure enough entropy before reseeding. In Pyth Entropy, reseed conceptually corresponds to adding new unpredictable bits from both participants for each request.	
Scaling	The scaling layer transforms raw 256-bit entropy into lottery numbers. Seed Derivation: For each set of numbers (main numbers, powerball), a unique seed is derived: seed[i] = keccak256(abi.encode(raw_entropy, i))	Compliant
Acceptable degree of freedom (DOF)	By degrees of freedom in a cryptographic PRNG context we mean parameters that can be chosen or tuned: Fortuna Degrees of Freedom Fortuna's design offers several tunable aspects: Number of entropy pools: Implementation choice (commonly 32). Block cipher choice: AES is typical, but others could be used. Reseed threshold: How much entropy triggers a reseed. Hash function for reseeding: Choice of secure hash (e.g., SHA-256). Pool scheduling rules: The application can adjust how often higher pools contribute. These parameters affect performance, security margins, and how quickly the system ingests entropy. Pyth Entropy Degrees of Freedom Pyth Entropy also has some configurable aspects: Provider key size and hash chain length. Reveal delay (confirmation time before providers can reveal). Callback gas limits and fees. Integration logic on the client side (e.g., how user entropy is incorporated). Verifiability constraints (e.g., how strict hash chain verification is). These design choices impact cost, latency, and security of randomness delivery on-chain.	Compliant
Usage	Suitable for usage with and without replacement.	Compliant

CONCLUSION

The results introduced in this test report refer exclusively to the product and/or sample(s) provided by the applicant. RiskCherry will not be held responsible for the validity of any and all references to third party documents included in this report as per the applicant's request.

The provided product has been tested using its English language version. All included test result deviations which do not explicitly conflict with the laboratory's final conformity verdict have been disclosed to the applicant as improvement recommendations. Based on all test results and compliance verdicts produced during this assessment, RiskCherry confirms that the product submitted by the applicant complies with the document(s) listed in section "Assessment Scope" which cover all relevant requirements issued by the Malta Gaming Authority (MGA).

All requirements which have a non-applicable verdict and a comment, stating that they fall outside of the scope of this test report, have not been tested and should not be considered as part of the compliance statement in the above paragraph. Only requirements related to random number generators have been tested. All requirements related to supplier's games and operator platform, security, system changes and any other non-RNG elements fall out of scope for this report.



Authorized by: Mihael Mladenov /Chief Operating Officer/ 07/08/2026