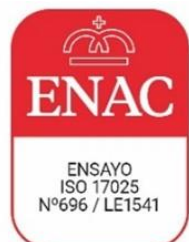


Evaluation Report for CT Interactive EOOD Random Number Generator RNG v6316

Manufacturer:	CT Interactive (Linux/Urandom)
ATF Report Number:	RNG.GRE.CATE-OL.1009.01.01
Document Number:	01
Date:	10 July 2024
Number of Pages:	12

BMM Spain Testlabs s.l.u.

The content of this document is strictly confidential. It has been prepared by BMM Spain Testlabs s.l.u. (BMM) exclusively for the perusal of CT Interactive EOOD and The Hellenic Gaming Commission and may not be disclosed to any other party without the prior written approval of CT Interactive EOOD.



GENERAL INFORMATION

Client name & Address:	CT Interactive EOOD 7 Kukush Str., 1345 - Sofia Bulgaria
Client Reference Number:	Submission request letter dated 21 st May 2024
Testing dates:	Start date: 18 June 2024 End date: 4 th July 2024
Product / Game Description:	RNG v. 6316 Software RNG SIGNATURES: See paragraph 2.2
Test Category:	RNG Evaluation
Jurisdictions Recommended:	Greece
Technical Standard used for Evaluation:	▪ Decision of the Minister of Finance number 67663 EΞ 2022/20.05.2022 (B '2483), which amended the Decision of the Minister of Finance number 79835 EΞ 2020/24.7.2020 entitled Adoption of Gaming Regulation on the Organization and Operation of online games of chance (B '3265, error corrections B 4441/2020) ▪ Decision of the Minister of Finance number No.58876 EΞ 2022/06.05.2022 which amended the Decision of the Minister of Finance number 79841 EΞ 2020 (B' 3266) entitled "Adoption of Regulation on the Technical Specification (TEP) for the Organization and Operation of online games of chance" published on 05/08/2020
Location where test was performed:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés - Barcelona (España)
Location where report was issued:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés - Barcelona (España)
Conclusion:	PASS
BMM Reference Number:	CATE-OL.1009
Method/Procedures used:	EURSAM-SPA-MO-41 v3.0
Consultant(s):	Gianni Piccioni

1. SCOPE OF EVALUATION.

CT Interactive EOOD requested BMM Spain Testlabs s.l.u., hereinafter referred to as BMM, to evaluate the products listed in section 2 for operation in the Greek Remote Gambling Market, accordingly with the Standards/Regulations described below:

- Decision of the Minister of Finance number 67663 EΞ 2022/20.05.2022 (B '2483), which amended the Decision of the Minister of Finance number 79835 EΞ 2020/24.7.2020 entitled Adoption of Gaming Regulation on the Organization and Operation of online games of chance (B '3265, error corrections B 4441/2020)
- Decision of the Minister of Finance number No.58876 EΞ 2022/06.05.2022 which amended the Decision of the Minister of Finance number 79841 EΞ 2020 (B' 3266) entitled "Adoption of Regulation on the Technical Specification (TEP) for the Organization and Operation of online games of chance" published on 05/08/2020

2. EVALUATION CHARACTERISTICS.

2.1. Source Code Review.

The following sections describe the implementation of the RNG in the source code.

2.1.1. SEEDING.

The RNG is cryptographically strong and uses the Fortuna algorithm, which changes the keys constantly and periodically.

2.1.2. CYCLING.

The RNG is cryptographically strong and does not cycle.

2.1.3. SCALING.

Scaling method does not introduce bias.

2.1.4. UNPREDICTABILITY.

The RNG is cryptographically strong and uses various sources of entropy to make the result unpredictable.

2.2. Statistical Testing.

Statistical tests were performed on the output from the RNG. Raw output from the RNG was subjected to a range of tests in the Empirical, Diehard and NIST test suites

Each test tests the hypothesis that the RNG is a random source of numbers. A "p-value" is produced for each test run, which is the probability that a truly random process would produce the same or a more extreme result. P-values are expected to be uniformly distributed between 0 and 1. The p-values for each test are evaluated using an Anderson-Darling test. This produces a single p-value, which is the probability that the individual p-values have been produced from a uniform distribution.

Finally, the p-values from each test in the same test suite are combined using the Holm-Bonferroni method to provide an overall p-value. This process adjusts each p-value to ensure that the overall probability of accepting the RNG as random matches the confidence interval used. The overall p-value, equal to the minimum of the adjusted p-values, is compared to a specific alpha value to determine if the RNG is accepted or rejected as being random for a specific confidence interval.

EMPIRICAL TESTS

The Empirical Tests are based on the tests described by Donald Knuth in The Art of Computer Programming Volume 2: Seminumerical Algorithms (1968, revised in 1997). They test sequences of numbers scaled to specific ranges.

Frequency Test	Counts of each number occurring across the sample set.
Serial Correlation Test	Counts of non-overlapping groups of numbers occurring together. Group sizes of two, three, and four are tested separately.
Runs Test	Counts of ascending and descending sequences of numbers. Note that this is a different test to the Runs Test in the Diehard and NIST Tests.
Gap Test	Counts of the size of gaps between successive occurrences of a given number. Each number in the range is tested separately.
Coupon Collector Test	Counts of sequence lengths required to complete a full set of each number in the range.
Subsequences Test	Similar to the Serial Correlation Test for pairs of numbers, except looking at numbers separated by a specific gap. Step sizes of 5, 10, 15, and 20 are tested separately.
Poker Test	The sequence is split into groups of five. The number of unique values in each group is counted.

Sample 1:

Test	P-values	95% Confidence	99% Confidence
Frequency Test	1.000000	PASS	PASS
Serial Correlation Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Gap Test	0.583222	PASS	PASS
Coupon Collector Test	1.000000	PASS	PASS
Subsequences Test	1.000000	PASS	PASS
Poker Test	1.000000	PASS	PASS
Overall	0.583222	PASS	PASS

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

Sample 2:

Test	P-values	95% Confidence	99% Confidence
Frequency Test	1.000000	PASS	PASS
Serial Correlation Test	0.856194	PASS	PASS
Runs Test	1.000000	PASS	PASS
Gap Test	1.000000	PASS	PASS
Coupon Collector Test	0.535097	PASS	PASS
Subsequences Test	0.585638	PASS	PASS
Poker Test	1.000000	PASS	PASS
Overall	0.535097	PASS	PASS

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

DIEHARD TESTS

The Diehard Tests are based on the test suite published by George Marsaglia in 1995. They test sequences of raw binary output from the RNG.

Binary Rank 32x32 Test	Matrices are created using 32 32-bit words. The ranks of the resulting matrices are counted.
Binary Rank 6x8 Test	Same as the Binary Rank 32x32 Test, except each matrix is formed using 6 values, each taking 8 bits from successive 32-bit words with a specific offset. All possible offsets are tested separately.
Birthday Spacings Test	26-bit values are taken from successive 32-bit words with a specific offset. The values are sorted, and the spacings between them calculated. The number of spacings of the same size are counted. All possible offsets are tested separately.
Bitstream Test	Blocks of 2^{18} values are treated as a stream of overlapping 20-bit values. The number of possible 20-bit values that are not found in each block is counted.
Count The 1's Stream Test	8-bit values are taken and assigned a "letter" based on the number of one's appearing in the binary representation of each value. Overlapping groups of 5 "letters" are counted.
Count The 1's Specific Test	Similar to the Count The 1's Stream Test, except 8-bit values are taken from successive 32-bit words with a specific offset. All possible offsets are tested separately.
Runs Test	Counts sequences of increasing and decreasing 32-bit words. Note that this is a different test to the Runs Test in the Empirical and NIST Tests.
Squeeze Test	A value of 2^{31} is repeatedly multiplied by 32-bit words, dividing by 2^{32} and taking the ceiling of the result each time. The number of successive words that are required to reduce the value down to 1 is counted. The value is reset to 2^{31} and the process is repeated.

Sample 1:

Test	P-values	95% Confidence	99% Confidence
Binary Rank 32x32 Test	1.000000	PASS	PASS
Binary Rank 6x8 Test	0.591772	PASS	PASS
Birthday Spacings Test	1.000000	PASS	PASS
Bitstream Test	0.935545	PASS	PASS
Count The 1's Stream Test	1.000000	PASS	PASS
Count The 1's Specific Test	0.585032	PASS	PASS
Runs Test	1.000000	PASS	PASS
Squeeze Test	1.000000	PASS	PASS
Overall	0.585032	PASS	PASS

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

Sample 2:

Test	P-values	95% Confidence	99% Confidence
Binary Rank 32x32 Test	0.367154	PASS	PASS
Binary Rank 6x8 Test	0.012529	FAIL	PASS
Birthday Spacings Test	1.000000	PASS	PASS
Bitstream Test	0.950484	PASS	PASS
Count The 1's Stream Test	1.000000	PASS	PASS
Count The 1's Specific Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Squeeze Test	0.731405	PASS	PASS
Overall	0.012529	FAIL	PASS

Conclusion: The RNG is **NOT ACCEPTED** as random at the 95% confidence interval.

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

NIST TESTS

The NIST Tests are based on the suite of tests released by the National Institute of Standards and Technology in Special Publication 800-22, Revision 1a (revised April 2010). They test sequences of raw binary output from the RNG.

Approximate Entropy Test	Similar to the Serial Test, count each possible m-bit value, except it does so for two adjacent m bit lengths and compares the two.
Block Frequency Test	Similar to the Frequency Test, except the data is split into equally sized blocks. The number of ones and zeroes in each block is counted.
Cumulative Sums Test	Random walks are created by converting the data to +1 / -1 for 1 / 0 respectively and summing consecutive values.
Discrete Fourier Transform Test	The data is transformed using a Discrete Fourier Transform. The number of peaks within the 95% threshold are counted.
Frequency Test	The number of ones and zeroes in the binary output is counted.
Linear Complexity Test	The length of the linear complexity of the random sequence is determined.
Longest Run of Ones Test	The data is split into equally sized blocks. The longest run of ones in each block is determined and counted.
Non-Overlapping Template Matchings Test	The data is split into equally sized blocks. Each block is searched for a specific pattern of bits and counted. A separate test is run for various bit patterns. Each bit pattern searched does not overlap with itself. That is, when the pattern is matched, the end of the pattern cannot be the start of another match.
Overlapping Template Matchings Test	Similar to the Non-Overlapping Template Matchings Test, except only one pattern is searched, which may overlap with itself.
Random Excursions Test	As with the Cumulative Sums Test, random walks are created by converting the data to +1 / -1 for 1 / 0 respectively and summing consecutive values. The number of times a given state is visited between returns to zero are counted. Separate tests are run for various states from -4 to +4, not including 0.
Random Excursions Variant Test	Similar to the Random Excursions Test, except the number of times the given state is visited is counted for the entire sequence. Separate tests are run for various states from -9 to +9, not including 0.
Rank Test	Matrices are created using 32 32-bit words. The ranks of the resulting matrices are counted. Note that this is fundamentally the same test as the

	Binary Rank 32x32 Test in the Diehard Tests, although the implementation may differ.
Runs Test	Runs of consecutive bits of the same value of various lengths are counted.
Serial Test	Counts of each possible m-bit values. Separate tests are run for various m bit lengths.
Universal Test	Distances between repeated patterns of bits are counted.

Sample 1:

Test	P-values	95% Confidence	99% Confidence
Approximate Entropy Test	1.000000	PASS	PASS
Block Frequency Test	1.000000	PASS	PASS
Cumulative Sums Test	1.000000	PASS	PASS
Discrete Fourier Transform Test	1.000000	PASS	PASS
Frequency Test	1.000000	PASS	PASS
Linear Complexity Test	1.000000	PASS	PASS
Longest Run of Ones Test	1.000000	PASS	PASS
Non-Overlapping Template Matchings Test	1.000000	PASS	PASS
Overlapping Template Matchings Test	1.000000	PASS	PASS
Random Excursions Test	1.000000	PASS	PASS
Random Excursions Variant Test	1.000000	PASS	PASS
Rank Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Serial Test	1.000000	PASS	PASS
Universal Test	1.000000	PASS	PASS
Overall	1.000000	PASS	PASS

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

Sample 2:

Test	P-values	95% Confidence	99% Confidence
Approximate Entropy Test	1.000000	PASS	PASS
Block Frequency Test	1.000000	PASS	PASS
Cumulative Sums Test	1.000000	PASS	PASS
Discrete Fourier Transform Test	1.000000	PASS	PASS
Frequency Test	1.000000	PASS	PASS
Linear Complexity Test	1.000000	PASS	PASS
Longest Run of Ones Test	1.000000	PASS	PASS
Non-Overlapping Template Matchings Test	1.000000	PASS	PASS
Overlapping Template Matchings Test	1.000000	PASS	PASS
Random Excursions Test	1.000000	PASS	PASS
Random Excursions Variant Test	1.000000	PASS	PASS
Rank Test	1.000000	PASS	PASS
Runs Test	1.000000	PASS	PASS
Serial Test	1.000000	PASS	PASS
Universal Test	1.000000	PASS	PASS
Overall	1.000000	PASS	PASS

Conclusion: The RNG is **ACCEPTED** as random at the 95% confidence interval.

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

2.3 EVALUATED SOFTWARE.

Product: RNG v6316					
File Name	Version	Location	Function	Digital Signature Type	Digital Signature
LinuxUrandom.pm	6316	Server	RNG	SHA1	D6893CAA6F2B2A8414C6 7BA2140F08C19D3C73CE
LinuxUrandomQueue.pm	6316	Server	RNG	SHA1	DEE2C8460E56767EAA7EE B776F176EECBA00CEF7
RNG.pm	6316	Server	RNG	SHA1	B5ADAA3D6C44132799960 B36889B2D9224553EF8

3. BMM EVALUATION PERFORMED.

BMM has tested and confirmed compliance of the RNG v.6316 against the appropriate applicable technical requirements for the Greek Remote Gambling market. BMM performed the following tests to confirm compliance to the relevant regulatory specifications:

GREECE REGULATIONS & ONLINE GAMING	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
RANDOM NUMBER GENERATOR				
ARTICLE 25 - RANDOM NUMBER GENERATOR CHARACTERISTICS				
25.1 GENERAL REQUIREMENTS FOR THE RANDOM NUMBER GENERATOR	25.1			
The random number generator (RNG) must have strong encryption at the time of submission. When more than one instance of a random number generator is used in the CIS, each instance must be assessed and certified separately. When the instances are identical, but require different implementation in the Game/application, each implementation must be assessed and certified separately. Analysis of the data and of the source code identification must demonstrate that any results of the random number generator used in determining the symbol/outcome of the Game:	☒	☐	☐	
	25.1			
(a) are statistically independent	☒	☐	☐	RNG uses various sources of entropy to be unpredictable
	25.1.a			
(b) are fairly distributed (within statistically expected limits) across their range	☒	☐	☐	
	25.1.b			
	☒	☐	☐	

GREECE REGULATIONS & ONLINE GAMING	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
(c) have passed various recognised statistical tests	25.1.c			See RNG Results for list of tests
(d) are strongly encrypted.	☒	☐	☐	RNG is cryptographically secure.
	25.1.d			
25.2 Checks applied	25.2			
The independent certification laboratory may use various applied tests to determine whether the random values generated by the random number generator successfully pass the desired 99% confidence level or not. Those tests may include, but are not limited to, the following:	☒	☐	☐	See RNG Results for list of tests
	25.2			
(a) chi-square test	☒	☐	☐	See RNG Results for list of tests
	25.2.a			
(b) equi-distribution (frequency) test	☒	☐	☐	See RNG Results for list of tests
	25.2.b			
(c) gap test	☒	☐	☐	See RNG Results for list of tests
	25.2.c			
(d) overlaps test	☒	☐	☐	See RNG Results for list of tests
	25.2.d			
(e) poker test	☒	☐	☐	See RNG Results for list of tests
	25.2.e			
(f) coupon collector test	☒	☐	☐	See RNG Results for list of tests
	25.2.f			
(g) permutation test	☐	☐	☒	See RNG Results for list of tests
	25.2.g			
(h) Kolmogorov-Smirnov test	☐	☐	☒	See RNG Results for list of tests
	25.2.h			
(i) agency criterion test	☐	☐	☒	See RNG Results for list of tests
	25.2.i			
(j) statistical order test	☒	☐	☐	See RNG Results for list of tests
	25.2.j			

GREECE REGULATIONS & ONLINE GAMING	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
(k) run tests (the pattern of occurrences should not be repeated)	☒	☐	☐	See RNG Results for list of tests
	25.2.k			
(l) interplay correlation test	☒	☐	☐	See RNG Results for list of tests
	25.2.l			
(m) serial correlation test potency and degree of serial correlation (outcomes must be independent of the previous Game)	☒	☐	☐	See RNG Results for list of tests
	25.2.m			
(n) sequence tests	☒	☐	☐	See RNG Results for list of tests
	25.2.n			
(o) Poisson distribution.	☒	☐	☐	See RNG Results for list of tests
	25.2.o			
NOTE: The independent certification laboratory must select the appropriate tests on a case-by-case basis, depending on the RNG being examined.				
25.3 Scaling				
The scaling method must not jeopardise the random number generator's encryption strength. Furthermore, the scaling method must safeguard the distribution of the scaled values. For example, if a 32-bit random number generator with a range of all the whole numbers within the closed interval [0, 232- 1] needs to be adjusted to the range of all the whole numbers within the closed interval [1,6], so that the scaled values can be used to simulate rolling a six-sided die, then each whole number in the scale's range must have the same theoretical frequency of occurrence. In the example given, if the theoretical frequency for each value is not equal, then the scaling method is considered to have a bias. Consequently, a compliant scaling method should have a bias equal to zero.	☒	☐	☐	Scaling method does not introduce bias
	25.3			
25.4 Hardware-based Random Number Generator				

GREECE REGULATIONS & ONLINE GAMING	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
Because of their nature, the performance of random number generators that use hardware may deteriorate over time. The failure of a hardware-based RNG could have serious consequences for the Game/application, e.g. Games could become predictable or have non-equitable distributions. Therefore, if a hardware-based RNG is used, there must be a dynamic/active, real-time tracking of the output, with a sample size large enough to allow several statistically robust tests, so that the Game is deactivated when an error is detected in the test result output.	☐	☐	☒	Not an hardware RNG
	25.4			
25.5 Software-based Random Number Generator	25.5			
The following requirements apply only to random number generators using software.	☒	☐	☐	RNG is an implementation of dev/urandom
	25.5			
25.5.1 Period				
The period of the RNG, in conjunction with the methods of implementing the RNG results, must be long enough to ensure that all independent combinations/variants of the result of the Games are possible for given Games/applications.	☒	☐	☐	RNG is cryptographically secure and can generate results in any range.
	25.5.1			
25.5.2 Seeding/re-seeding				
The Seeding/Re-seeding methods must ensure that all the values of the seed used to start or initialise the random number generator are determined in such a way as not to jeopardise the cryptographic security of the random number generator.	☒	☐	☐	Fortuna algorithm changes the keys constantly and periodically.
	25.5.2			
25.5.3 Background cycling/activity				
To ensure that the results of the RNG cannot be predicted, the appropriate background activity	☒	☐	☐	

GREECE REGULATIONS & ONLINE GAMING	PASS	FAIL	N/A	NOTES
	EXTERNAL REF #			
must be applied between Games. When the result of a Game consists of multiple RNG mapped values, the background activity must be applied for the whole duration of the Game (i.e. between the selection of each mapped RNG value) to ensure that the result of the Game does not consist of consecutive mapped RNG results. Background operation must be activated randomly, without intervention, so as to prevent any prediction.	25.5.3			Fortuna algorithm changes the keys constantly and at each request. Various sources of entropy are used.

4. ADDITIONAL INFORMATION/OBSERVATIONS.

N/A

5. CONCLUSION.

According to the test results¹, BMM Spain Testlabs s.l.u. confirms that the item submitted for testing is compliant with all the relevant technical requirements listed in section 3.

Yours sincerely,

Rubén Baptista

SVP Operations EURSAM

¹ The results included in this document refer exclusively to the sample tested, such as it is described in the corresponding section.

This test report may not be reproduced, other than in full, except with the prior written permission of the issuing BMM Spain Testlabs, s.l.u.