

Evaluation Report for Kiverly Ltd Random Number Generator libccr version 1.1.0

Manufacturer: Kiverly Ltd
ATF Report Number: RNG.UK.SGTV-OL.1001.01.01
Document Number: 01
Date: 4 October 2023
Number of Pages: 7

BMM Spain Testlabs s.l.u.

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. 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 Kiverly Ltd and the UK Gambling Commission and may not be disclosed to any other party without the prior written approval of Kiverly Ltd.



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)

t: +34 93 143 3862

business no. B64622251

v.2.8 2023/02/07

bmm.com

GENERAL INFORMATION

Client name & Address:	Kiverly Ltd 28 Oktovriou, 367, MEDITERRANEAN COURT, 1st floor, Flat Office A5 3107 Limassol Cyprus
Client Reference Number:	Client Submission Letter Dated 28 th September 2023
Testing dates:	Start date: 2 nd October 2023 End date: 2 nd October 2023
Product / Game Description:	libccr v 1.1.0 Software RNG
Platform Name and Version	N/A
Jurisdictions Recommended:	United Kingdom
Technical Standard used for Evaluation:	Remote Gambling and Software Technical Standards, February 2021
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:	SGTV-OL.1001
Method/Procedures used:	EURSAM-SPA-MO-41 v2.9
Consultant(s):	Giacomo Quaranta

1. SCOPE OF EVALUATION.

Kiverly Ltd requested BMM Spain Testlabs s.l.u., hereinafter referred to as BMM, to evaluate the products listed in section 2 for operation in the United Kingdom Remote Gambling Market.

- Remote Gambling and Software Technical Standards, February, 2021

2. PRODUCT CHARACTERISTICS.

BMM examined the RNG source code and performed statistical tests on the output from the RNG.

2.1. SOURCE CODE REVIEW.

The RNG's primary source of randomness is the `RAND_bytes` function from OpenSSL. This is used to provide a random strings of 40 characters. This is a cryptographically secure RNG, using the AES-256 CTR-DRBG secure algorithm with entropy drawn from system sources. This string is combined with a seed provided by the player. The resulting string is hashed with the SHA512 algorithm using the SHA512 function from OpenSSL to produce a 128-character hex string (512-bit) output. This is used to generate numbers in the interval $[0, 2^{64} - 1]$. However the RNG finally produce numbers in the interval $[0, 2^{28} - 1]$.

2.1.1 SEEDING

Seeding is performed at each round using `RAND_bytes` function from OpenSSL.. The OpenSSL RNG is seeded from numerous system sources of entropy.

2.1.2 CYCLING

The RNG is crypto-secure

2.1.3 SCALING

No scaling methods are used or provided by the RNG for producing random numbers in smaller usable ranges. The RNG can generate random numbers in the interval $[0, 2^{64} - 1]$. However just random numbers in the interval $[0, 2^{28} - 1]$ are actually generated.

2.1.4 UNPREDICTABILITY

The RNG is unpredictable.

2.2. STATISTICAL TESTING.

Statistical tests were performed on the output from the RNG. Both Raw outputs, in the range $[0, 2^{64} - 1]$ and $[0, 2^{28} - 1]$ from the RNG were subjected to a range of tests in Diehard and NIST test suites. Their results were finally combined.

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.

Diehard Tests

Test	P-values	95% Confidence	99% Confidence
Binary Rank 32x32 Test	1.000000	PASS	PASS
Binary Rank 6x8 Test	1.000000	PASS	PASS
Birthday Spacings Test	1.000000	PASS	PASS
Bitstream Test	1.000000	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	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.

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	32-bit words are taken as values, sorted, and the spacings between them calculated. The number of spacings of the same size are counted.
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.

NIST Tests

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.

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.

2.3. EVALUATED SOFTWARE.

Product: <i>libccr</i>					
File Name	Version	Location	Function	Digital Signature Type	Digital Signature
libccr.so	<i>1.1.0</i>	<i>Server</i>	RNG	SHA1	6F7CC113DF0F7FE8A7B844FF4639B3B26E0AAF0B

3. BMM EVALUATION PERFORMED.

BMM has tested and confirmed compliance of the Software RNG libccr v1.1.0 against the appropriate applicable technical requirements for the United Kingdom Remote Gambling market. BMM performed the following tests to confirm compliance to the relevant regulatory specifications:

Remote Gambling and software technical standards, February 2021.	RESULTS			Observations / Comments
	PASS	FAIL	N/A	
Table 1.				
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, though, for example, statistical analysis using generally accepted tests and methods of analysis. Adaptive behaviour (i.e. a compensated game) is not permitted	☒	☐	☐	

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 Regulations listed in section "1" of this report.

Yours sincerely,

Rubén Baptista
SVP Operations ERSAM

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