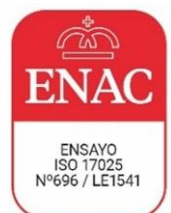


Evaluation Report for
Amarix B.V.
AMARIX-RNG
Version 1.0.0

Manufacturer: Amarix B.V.
ATF Report Number: RNG.CRO.RES-OL.1001.01.01
Document Number: 01
Date: 25 July 2024
Number of Pages: 16

BMM Spain Testlabs s.l.u.

The content of this document is strictly confidential. It has been prepared by BMM Testlabs (BMM) exclusively for the perusal of Amarix B.V. and Ministarstvo Financija, Porezna Uprava - Središnji ured and may not be disclosed to any other party without the prior written approval of Amarix B.V.



GENERAL INFORMATION

Name of petitioner	Andreas Christou DIRECTOR
Name and address of the petitioner	Amarix B.V. Schottegatweg Oost 10 Unit 1-9, Bon Bini Business Center, Curaçao a.christou@amarix.com
Reference Number:	Client Submission Letter Dated 30 th April 2024
Testing dates:	Start date: 30 th April 2024 End date: 6 th June 2024
Category of evaluation	Category 0
Type of evaluation	Evaluation of a technical Project for an Online Platform
Product Description:	AMARIX-RNG Version 1.0.0 RNG software
Jurisdictions Recommended:	Croatia
Technical Standard used for Evaluation	▪ Croatia, Gaming Law, as published in the official gazette of the Republic of Croatia 'Narodne novine' No. 87/09 (consolidated text, Official Gazette 87/09, 35/13, 158/13, 41/14, 143/14). ▪ Ordinance on interactive online casino gaming, published in the Official Gazette of the Republic of Croatia "Narodne novine" N° 78/10. ▪ Croatia, U2, Guidelines for Certification of Internet Casino Systems.
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 of Evaluation:	PASS
BMM Reference Number:	RES-OL.1001
Method / Procedures used:	EURSAM-SPA-MO-41 v3.0
Test Engineer:	Alexander Guerra
Certifying Engineer: Name and Position	Rubén Baptista SVP Operations EURSAM

1. SCOPE OF EVALUATION.

Amarix B.V. requested BMM to evaluate AMARIX-RNG v1.0.0, the remote online platform/game for operation in the relevant below Croatian market:

- Croatia, Gaming Law, as published in the official gazette of the Republic of Croatia 'Narodne novine' No. 87/09 (consolidated text, Official Gazette 87/09, 35/13, 158/13, 41/14, 143/14).
- Ordinance on interactive online casino gaming, published in the Official Gazette of the Republic of Croatia "Narodne novine" № 78/10.
- Croatia, U2, Guidelines for Certification of Internet Casino Systems.

2. EVALUATION CHARACTERISTICS.

2.1. PRODUCT DESCRIPTION.

The software RNG in the system is the RNG service. It is hosted in a Kubernetes cluster on a virtual server in the data center. The RNG service is written in Java 17 and uses the org.apache.commons:commons-rng-simple:1.5 library from the Maven Central repository.

When the service is launched, 64 random bytes are read from the source /dev/urandom, which are used as seeds for the ISAAC algorithm. With each request for a random number, the RNG service returns 32 random bytes generated by the ISAAC algorithm. This number is used as a seed to the next steps.

Each game also has a salt string specified in the configuration. The obtained bytes undergo the hash function: hash sha256 in loops of 1000 iterations. The hash is combined with the clientSeed and nonce received from the player to obtain the random number. The result string is a 64-character hex string (256-bit) output to be used directly by the game logic to produce game outcomes.

2.2. EVALUATED SOFTWARE.

Product: AMARIX-RNG v1.0.0					
File Name	Version	Location	Function	Digital Signature Type	Digital Signature
rng-sbai-certified.jar	1.0.0	Server	RNG	SHA-1	98846A088426F85600EE 32DEF1AB6A6AE90B3916
rng-sbai-certified-sources.jar	1.0.0	Source	RNG source	SHA-1	8354EC44F14D0AC0FA12 05F75B7A665A1D9F08A7

3. BMM EVALUATION PERFORMED.

3.1. SOURCE CODE REVIEW.

BMM examined the RNG source code and performed statistical tests on the output from the RNG. The relevant file(s) used are listed in section 2.2.

3.1.1. SEEDING.

The ISAAC algorithm (seeded from the source /dev/urandom) produces a random seed.

3.1.2. CYCLING.

The algorithm is seeded each 1000 requested numbers.

3.1.3. SCALING.

The algorithm doesn't produce any scaling algorithm.

3.1.4. UNPREDICTABILITY.

The RNG uses sha256 to produce unpredictable outcomes.

3.2. 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. Appendix A describes the tests run in each test suite.

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.

3.2.1. 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.

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	0,909765	PASS	PASS
Coupon Collector Test	1,000000	PASS	PASS
Subsequences Test	1,000000	PASS	PASS
Poker Test	1,000000	PASS	PASS
Overall	0,909765	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.

3.2.2. 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	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.

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	0,071261	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	0,071261	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.

3.2.3. 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.

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	0,146020	PASS	PASS
Serial Test	1,000000	PASS	PASS
Universal Test	1,000000	PASS	PASS
Overall	0,146020	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.

3.3. EVALUATION OF THE TECHNICAL REQUIREMENTS.

BMM has tested the new Amarix B.V. software AMARIX-RNG v1.0.0, against the relevant requirements of the Croatian online market:

U2, Guidelines for Certification of Internet Casino Systems, v1.0 issued on 27th of March 2015	Results		
	Pass	Fail	Observations
C.1. Operation system			
<u>C.1.1. Individual games</u> Players can play a game individually, in interaction with a system, without a direct representative of the operator. The player must be able to access the system via the Internet.	☐	☐	N/A. Just RNG software evaluation.
<u>C.1.2. Electronic payment receipt</u> Electronic Payment Receipt is an electronic record of payment for a game, marked with player ID number from the player's account in the operator's central system. The operator shall enable the printing of this record.	☐	☐	N/A. Just RNG software evaluation.
<u>C.1.3. Storage of Pay-in and Pay-out</u> It is necessary to determine that the Operating System records all payments (Pay-in and Pay-out) of the i-account. It is necessary to determine all financial transactions to the i-account and from the i-account. <u>Financial transactions include:</u> Payment to the i-account for all ways of receiving payments: Payment by activation ticket - so-called "prepaid", Payment by debit or credit cards, Payments by other means of electronic payments, Standard bank transfer or internet bank transfer Pay-outs from i-account for all ways of payment: ▪ At the Cashier of casino ▪ By means of electronic money transfer system ▪ To the registered player's transaction account. Payments in the game. Pay-outs to the i-account.	☐	☐	N/A. Just RNG software evaluation.

U2, Guidelines for Certification of Internet Casino Systems, v1.0 issued on 27th of March 2015	Results		
	Pass	Fail	Observations
Bonuses awarded to players. Revisions and corrections Any other financial transactions that are not included in the previous list. It is necessary to identify and record the exact location of the data record of the Financial transactions from the Operating System.			
<u>C.1.4. Immutability of the information received</u> It is necessary to determine that the immutability of financial transactions referred in C1.3 of the Operation System are guaranteed. Immutability of the received data can be ensured through the implementation of data delete protection on the database level. Any change of data must be recorded as a new record. At the same time, it is preserved the previous record that does not change. Immutability of the information received must be also ensured by storing copies of daily financial data in an irreversible (permanent/indelible) media (CD, DVD or other permanent storage media). Such copies of data on indelible media shall be properly labeled and stored.	☐	☐	N/A. Just RNG software evaluation.
<u>C.1.5. Server location</u> The Operating System is located on the Croatian territory. The Software System is located on the Croatian territory. While analyzing the modules contained in the operating system, it is necessary to detect the modules from the Operation System Sketch (Skica Sustava Priređivanja - SSP) from "Instructions for Online Casino Operators" - U1.	☐	☐	N/A. Just RNG software evaluation.
<u>C.1.6. Operating System Sketch</u>	☐	☐	N/A. Just RNG software evaluation.

U2, Guidelines for Certification of Internet Casino Systems, v1.0 issued on 27th of March 2015	Results		
	Pass	Fail	Observations
During the certification process it is necessary to determine compliance of the Operating System Sketch (SSP) with the factual situation of the Operating System. The SSP is defined by the "Instructions for Online Casino Operators" (U1) and shall be provided by the operator for the purpose of certification. It is necessary to determine that the Operating System of the organizer has as minimum all modules defined in the SSP template. It is necessary to determine the system address (SA) and the physical address (FA) of each module.			
C.2. Games			
<u>C.2.1. Compliance games</u> It is necessary to determine that the RNG certificate and the games certificate are consistent with the facts. It is necessary to determine that each game from the Operation System has a corresponding certificate.	☐	☐	N/A. Just RNG software evaluation.
<u>C.2.2. Location of the games</u> It is necessary to determine the System Address (SA) and Physical Address (FA) address of game modules and their compliance with the Operating System Sketch (SSA).	☐	☐	N/A. Just RNG software evaluation.
C.3. Registration and identification of players			
<u>C.3.1. Registration of players</u> Registration of players includes download and store data about the player. For the purposes of registering the player must give the following information: 1. Name and surname, 2. Address, 3. ID,	☐	☐	N/A. Just RNG software evaluation.

U2, Guidelines for Certification of Internet Casino Systems, v1.0 issued on 27th of March 2015	Results		
	Pass	Fail	Observations
4. Date of birth, 5. e-mail address, 6. The preferred username, 7. The preferred password (password) that meets the necessary level of safety standards, 8. The number of only one transaction account for the purpose of payment. Players can be registered on the basis of the agreement concluded with the operator in the casino or by means of the operator's web site.			
<u>C.3.2. Identification of the age of majority</u> Each registered player has to be identified and has to be determined the age of majority (at least 18 years). Identification of players is a process whereby the truthfulness of players' data and their full age are determined by means of data verification via electronic services of the Tax Administration. Players' full age can also be determined via the electronic payment system by verifying the debit or credit card holder.	☐	☐	N/A. Just RNG software evaluation.
<u>C.3.3. Storage of information on players</u> It is necessary to establish a System Address (SA) and Physical Address (FA) of the module with data from the player registration and its compliance with the Operation System Sketch (SSA).	☐	☐	N/A. Just RNG software evaluation.
C.4. Player's Virtual Account (e-account)			
<u>C.4.1.</u> The record of pay-in and pay-out transactions on i-account Payment of funds to the i-account can be: ▪ Payment by activation ticket - so-called "prepaid", ▪ Payment by debit or credit cards, ▪ Payments by other means of electronic payments,	☐	☐	N/A. Just RNG software evaluation.

U2, Guidelines for Certification of Internet Casino Systems, v1.0 issued on 27th of March 2015	Results		
	Pass	Fail	Observations
Standard bank transfer or internet bank transfer Winnings from interactive online casino games gained by a player shall automatically be transferred by the operator to the player's virtual account (I-account).			
<u>C.4.2. Prohibition of payment</u> It shall not be permitted to operators to capture a payment for interactive online casino gaming from players who do not have sufficient funds on their account (I-account) to cover the payment amount.	☐	☐	N/A. Just RNG software evaluation.
<u>C.4.3. The records of payment transactions from the e-account</u> Payments from the i-account can be: - At the Cashier of the casino - By means of electronic money transfer system - To the registered player's transaction account.	☐	☐	N/A. Just RNG software evaluation.
<u>C.4.4. The records on transactions</u> The system must record all transactions, pay-in and pay-out (winnings).	☐	☐	N/A. Just RNG software evaluation.
<u>C.4.5. Location of the server with games</u> Server with the games must be located in the Republic of Croatia. It is necessary to determine the system (SA) and physical (FA) addresses of the game module and its compliance with Operating System Sketch (SSA).	☐	☐	N/A. Just RNG software evaluation.
C.5. Principles of Responsible Gaming			
<u>C.5.1. Determination of the maximum amounts</u> Registered players can, in writing or via e-mail, establish for the operator the highest amount which can be paid during a certain period of time, i.e. establish the highest amount of loss which they can afford during a certain period of time.	☐	☐	N/A. Just RNG software evaluation.

U2, Guidelines for Certification of Internet Casino Systems, v1.0 issued on 27th of March 2015	Results		
	Pass	Fail	Observations
C.5.2. Self-exclusion Players can in written form demand to be excluded from the game for a defined period of time. Operators shall exclude from the game players who within three days confirm their request for self-exclusion.	☐	☐	N/A. Just RNG software evaluation.
C.5.3. Revocation of the maximum amount of play and self-exclusion Registered players can cancel the highest amount for game, the ceiling of loss or self-exclusion in writing form or via e-mail.	☐	☐	N/A. Just RNG software evaluation.
C.5.4. Information on payments and redemptions Information about payments for interactive online casino gaming and winnings paid out shall be available to players at all times.	☐	☐	N/A. Just RNG software evaluation.
C.5.5. The implementation of standards for the protection of players Operators shall appoint a person to carry out standards for the player protection, who is responsible for the implementation of protection, for training and improvement of player protection standards.	☐	☐	N/A. Just RNG software evaluation.
C.5.6. Information on helping The organizer is required to the participants in the game to make available information on where they can get help in case of problems associated with excessive playing.	☐	☐	N/A. Just RNG software evaluation.

Gaming Law, This Act was published in the official gazette of the Republic of Croatia 'Narodne novine' No. 87/09	Results		
	OK	Fail	Observations
Disbursements at the Slot Machines			
Article 64. The slot machines shall be designed in such a way that on the total number of programmed combinations, 80% of the value of the receipts for the participation in the games of chance is disbursed to the players, whereas the input and output are recorded.	☐	☐	N/A. Just RNG software evaluation.

Ordinance on interactive online casino gaming No.78/10	Results		
	OK	Fail	Observations
V. Types of games and rules			
17.1 For each type of interactive online casino games, the operator shall adopt rules that are in compliance with good business practice and international rules, which shall be applicable after the authorization of the Ministry of Finance	☐	☐	N/A. Just RNG software evaluation.
17.2 Rules of games of chance shall be written in Croatian, Latin script, and translated into at least two world languages, and they shall always be available to the players on the web site where the interactive online casino games will be organized	☐	☐	N/A. Just RNG software evaluation.
17.3 Operators of interactive online casino games shall have an option to combine a real game and an online game by showing individual games for which they have the authorisation of the Ministry of Finance on their web page in real time, i.e. live (so called casino room).	☐	☐	N/A. Just RNG software evaluation.
17.4 Operators shall have the right to award bonuses to players in the form of virtual points, depending on the frequency of playing, amount of deposit, VIP status previously gained by the player and the like.	☐	☐	N/A. Just RNG software evaluation.
VI. Software and equipment requirements and system and games certification			

Ordinance on interactive online casino gaming No.78/10	Results		
	OK	Fail	Observations
18.1 The certainty of an event of chance shall not be influenced or forced, i.e. shall be controlled by no means other than numeric values obtained in a certified manner and via certified random number generator (RNG) together with the rules of game.	☒	☐	
18.2 Random number generator (RNG) and its methodology shall be based on pseudorandom algorithm of number generation. When multiple RNGs are used in a system, each variation shall be separately evaluated and certified.	☒	☐	

4. DESCRIPTION OF THE PLACE, EQUIPMENT AND DATES OF EVALUATION.

The evaluation has been done by BMM Spain Testlabs. Samples have been generated using Java and statistical testing has been performed using the RNG Tester software.

5. ADDITIONAL INFORMATION/OBSERVATIONS.

N.A.

6. 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 EUSAM

¹The 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.