Certification Report: ITL2401101

Eyecon Alderney Limited

Random Number Generator Certification Report
Gibraltar Gambling Commission

04 July 2024

Certification Report: ITL2401101

1. Test Laboratory details

Nº	Description	Details
1.	Contact Details of Test Laboratory	iTech Labs Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia URL: www.itechlabs.com E-mail: info@itechlabs.com
2.	Physical location of where testing was performed	iTech Labs, Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia
3.	Date Commenced	30 May 2024
4.	Date Completed	04 July 2024
5.	Scope of Work	This RNG was previously certified. This is a recertification.
6.	Result	Passed all tests, subject to Section 5 Final declaration and conformity, Item 1 Conditions.
7.	Other	None
8.	Test Supervisor Signature:	 _____ Alvin Rizaldi, Chief Executive Officer, iTech Labs

2. Executive summary

2.1 General Information

Nº	Description	Details
1.	Identification	Eyecon Alderney Limited RNG
2.	Type of system	Online Casino
3.	Games using this RNG	Non-card games: Slot and Instant games
4.	Target Jurisdiction	Gibraltar
5.	Guidelines used for testing	Remote Technical and Operating Standards for the Gibraltar Gambling Industry - Gambling Commissioner's Guidelines - v.1.1.0.
6.	Software provider	Name: Eyecon Alderney Limited Address: Inchalla, Le Val GY9 3UL Alderney URL: https://play.eyecongames.com/, https://play.eyeconalderney.gg Contact: Helen Ackrill Email: helen.ackrill@ackrill.gg
7.	Operator details	Operator Name: N/A Address: N/A URL: N/A Contact: N/A Email: N/A

2.2 Description of RNG

2.2.1 Software Details

Nº	Description	Details
1.	RNG type	Pseudo Random Number Generator (PRNG)
2.	Implementation language	Java

Nº	Description	Details
3.	RNG version number	2.0.0
4.	RNG build number	2.0.1
5.	Superseded RNG	This RNG was previously certified. This is a recertification.
6.	RNG algorithm	SHA1 PRNG
7.	Period of algorithm	2^160
8.	Dimension of numbers from algorithm	32 bit integer with the interval 0 to (2^32-1)
9.	Seeding	Auto-seeded by the Java runtime library prior to first use. The seeding is done using system entropy sources from the OS.
10.	Reseeding	No reseeding
11.	Library name and version	The RNG uses the SecureRandom class from the standard Java runtime library. Hence this RNG certification is restricted to Amazon Corretto Java runtime library version 8.0 to 22.x (Current version).
12.	Real time/dynamic monitoring	Every 1 minute random number are drawn, the monitoring tests are automatically initiated at 99% confidence interval. If a failure is observed, another chi-square test is initiated immediately to check if the failure is persistent. If 3 such re-initiated test attempts also show a failure, then the RNG is marked as Failed. When the test results retrieved by monitoring system indicate a failure, the RNG health endpoint must be monitored for an additional amount of time equal to collecting another window of sample results. Continued failure results in the system being placed into maintenance mode until failures have been investigated further and the RNG has been identified as faulty or the RNG has been replaced with an alternative implementation. The game is stopped when it is disabled manually.
13.	Operating system	Linux
14.	Environmental particulars	Platform supplier hosting the RNG: Eyecon Alderney Limited Platform version hosting the RNG: StellaV GS 3.16.0
15.	Files and SHA-1 hashes	Refer to Section 2.3 Critical Components of RNG Table 1 and Table 2 below for the list of hashes of source code files and binaries (if applicable) of the RNG.

2.2.2 Hardware Details

Not Applicable, software RNG.

2.3 Critical Components of RNG

Table 1: List of RNG source files

No	File Name
01	SHA1PRNGAdapter.java

Table 2: SHA-1 Signature of executables

File Name	Size (bytes)	SHA-1
SHA1PRNGAdapter.class	1,598	53ef6787f3da368ace3d0d878fa393edceb2fb5f

2.4 Scope of Testing

Nº	Description	Details
1.	Vendor supplied output testing	Not Applicable
2.	Test Laboratory generated output from vendor supplied source	Source files were compiled by iTech Labs using the source code supplied by the customer. Refer to Section 2.3 Critical Components of RNG.
3.	Source code review	The source code review verified that the implementation of the RNG is in accordance with the technical requirements. This includes, but is not limited to: a) Identification of algorithm; b) Security of internal state, seeding and re-seeding, thread safety; c) Scaling for Slot and Instant games; d) Dynamic monitoring
4.	Statistical tests	The statistical tests undertaken by iTech Labs are: a) Diehard tests b) Chi-square tests
5.	Theoretical basis of algorithm and supporting crypto-analysis evidence	Literature is readily available, describing the theoretical basis of the algorithm (refer to Section 2.2) SHA1PRNG: http://docs.oracle.com/javase/1.5.0/docs/guide/security/CryptoSpec.html#AppA Wikipedia: http://es.wikipedia.org/wiki/SHA1PRNG

2.5 Limitation of use of RNG

Nº	Description	Details
1.	Acceptable degrees of freedom (DOF) permitted	Acceptable DOF's are listed in Section 3.1 Item 5 (below).
2.	Dependency on operating system functionality	None
3.	Library-based implementation	The RNG uses the SecureRandom class from the standard Java runtime library. Hence this RNG certification is restricted to Amazon Corretto Java runtime library version 8.0 to 22.x (Current version).
4.	Other	None

3. Detailed test results

3.1 Tests methodology

The testing methodologies listed below were used to ensure the RNG complies with the relevant jurisdictional technical requirements and the scope of work. The following details of slot game are from the testing conducted during the previous round of certification. Additional tests were performed for Instant game in this round of recertification.

Nº	Test Performed	Test Methodology	Result
1.	Review of RNG documentation	Review of RNG documentation was conducted to understand the implementation of RNG in the gaming system.	Comply
2.	Research conducted about RNG algorithm/ hardware	Research conducted about RNG the algorithm to ensure there is no publicly known weakness or vulnerabilities associated with the RNG under evaluation.	Comply
3.	Review of source code	Review of source code was conducted to verify that the implementation of the RNG is in accordance with the technical requirements.	Comply

Nº	Test Performed	Test Methodology	Result
4.	Statistical testing of raw output of RNG.	Marsaglia's diehard tests were applied to 80 million bits of raw 32 bit random numbers generated by the algorithm. The following diehard tests were conducted on 2 sets of 80 million bits; i. BIRTHDAY SPACINGS ii. OVERLAPPING 5-PERMUTATIONS iii. BINARY RANK TEST for 31x31 matrices iv. BINARY RANK TEST for 32x32 matrices v. BINARY RANK TEST for 6x8 matrices vi. BITSTREAM TESTS ON 20-BIT Words vii. BITSTREAM TESTS OPSO, OQSO, DNA viii. COUNT-THE-1's IN A STREAM OF BYTES ix. COUNT-THE-1's IN SPECIFIC BYTES x. PARKING LOT TEST xi. MINIMUM DISTANCE TEST xii. THE 3DSPHERES TEST xiii. THE SQUEEZE TEST xiv. OVERLAPPING SUMS TEST xv. RUNS TEST xvi. CRAPS TEST	Comply Refer Section 4.1 for results.
5.	Statistical testing of scaled / shuffled data	Chi-square tests/ Frequency Distribution tests were conducted for Slot games: DOF for Slot games: (Reel Length = 29): 28 (Reel Length = 30): 29 (Reel Length = 32): 31 (Reel Length = 33): 32 (Reel Length = 34): 33 (Reel Length = 35): 34 (Reel Length = 36): 35 (Reel Length = 37): 36 (Reel Length = 38): 37 (Reel Length = 39): 38 (Reel Length = 40): 39 (Reel Length = 41): 40 (Reel Length = 42): 41 (Reel Length = 43): 42 (Reel Length = 44): 43 (Reel Length = 45): 44 (Reel Length = 46): 45 (Reel Length = 48): 47 (Reel Length = 49): 48 (Reel Length = 52): 51 (Reel Length = 57): 56 (Reel Length = 59): 58 (Reel Length = 60): 59 (Reel Length = 64): 63 (Reel Length = 67): 66 (Reel Length = 68): 67 (Reel Length = 69): 68 (Reel Length = 71): 70 (Reel Length = 72): 71 (Reel Length = 73): 72 (Reel Length = 75): 74 (Reel Length = 76): 75 (Reel Length = 78): 77 (Reel Length = 80): 79	Comply Refer Section 4.2 for results

Nº	Test Performed	Test Methodology	Result
		(Reel Length = 88): 87 (Reel Length = 90): 89 (Reel Length = 93): 92 Weighted Single Number* (5 elements, Sum of weights=120): 4 Weighted Single Number* (11 elements, Sum of weights=1000): 10 Weighted Single Number* (12 elements, Sum of weights:3170): 11 Weighted Single Number* (12 elements, Sum of weights=39790): 11 Weighted Single Number* (12 elements, Sum of weights=2613): 11 Weighted Single Number* (5 elements, Sum of weights=100): 4 Weighted Single Number* (8 elements, Sum of weights=1200): 7 DOF for Instant games: (Range = 2): 1 Weighted Single Number* (17 elements, Sum of weights=10145): 16 Weighted Single Number* (14 elements, Sum of weights=3946): 13 Weighted Single Number* (18 elements, Sum of weights=57883): 17 Weighted Single Number* (17 elements, Sum of weights=50383): 16 Weighted Single Number* (7 elements, Sum of weights=1032): 6 * There is no concept of "range" for the weighted test. The scaling range used by the RNG would be the sum of weights provided as inputs. The DOF is (no of elements -1) because the result of each draw has possible values equal to total number of elements (i.e. the function call picks one index out of total number of elements with elements having probabilities equal to the weight values.	
6.	Other	The above test results apply to the code provided by the customer as specified in section 2.3.	-

Note: Evaluation was conducted at iTech Labs facilities in Australia and India.

3.2 Compliance to technical standards

Nº	Requirement Description	Results	Comments
11.	**Randomness**		
11.1	**RNG and Game Randomness**		
	(1) Licence holders should be able to demonstrate the fairness and randomness of all games to the Gambling Commissioner without any undue delay.	Comply	RNG complies with the requirements of the standard. Game testing is not included in the scope of work for this certification.
	(2) The output obtained through the use of the RNG in games shall be proven to: (a) Be statistically independent. (b) Be uniformly distributed over their range. (c) Pass various recognised statistical tests intended to demonstrate a) and b) above and the absence of patterns. (d) Be unpredictable without knowledge of the algorithm, its implementation, and the current seed value (all of which should be secure). (e) be random and distributed in accordance with the rules and expected probabilities of the game.	Comply	
11.2	**Mechanical RNGs**		
	(1) For games that use the laws of physics to generate game outcomes ("mechanical RNGs")	Not applicable	Mechanical RNGs are out of the scope of work for this certification.

Nº	Requirement Description	Results	Comments
	the mechanical RNG should also meet the following guidelines: (a) Components should be constructed of materials that will not degrade before their scheduled replacement lifecycle. (b) The properties of the items used should not be altered. (c) Customers should not have the ability to interact with, come into physical contact with, or manipulate the mechanics of the game.		
11.3	**RNG Failure**		
	(1) Systems should be in place to quickly identify any failure of the RNG (for example, if a short sequence is repeated, or if the output is a constant flow of the same value).	Comply	Every 1 minute random number are drawn, the monitoring tests are automatically initiated at 99% confidence interval. If a failure is observed, another chi-square test is initiated immediately to check if the failure is persistent. If 3 such re-initiated test attempts also show a failure, then the RNG is marked as Failed. When the test results retrieved by monitoring system indicate a failure, the RNG health endpoint must be monitored for an additional amount of time equal to collecting another window of sample results. Continued failure results in the system being placed into maintenance mode until failures have been investigated further and the RNG has been identified as faulty or the RNG has been replaced with an alternative implementation. The game is stopped when it is disabled manually.
	(2) In the event of an RNG failure, games that rely upon that RNG should be made unavailable for gambling until the failure is rectified or the RNG replaced.	Comply	The lockdown mechanism of the RNG failure is verified. Making the games unavailable upon such a lockdown is platform / operator's responsibility.
11.4	**Verifiably Fair**		
	(1) A licence holder's remote gambling services should be verifiably fair to the customer in terms of the performance of the facility in accordance with the published rules and terms and conditions. The licence holder's website(s) and game client (where applicable) should have a "fairness"/"fair gambling" content that: (a) Informs the customer of the measures taken to ensure fair gambling such as the in-house and/or external quality management and/or testing that the licence holder undertakes to certify the fairness and reliability of its product(s). (b) Provides access to copies of any certificates by ATFs and/or other bodies with respect to information security, RNG (randomness, fairness, integrity etc.)	Not Applicable	Not within the scope of work. Licence responsibility to display the content required to verify fairness.

Nº	Requirement Description	Results	Comments
	(c) Provides a Frequently Asked Questions ("FAQ") section specific to gambling fairness.		
	(2) The home page, "about us" page and the customer registration page(s) of the licence holder's website(s) should display a link to the licence holder's "fairness"/"fair gambling" gambling content.	Not applicable	Not within the scope of work. Licence responsibility to display the required links on the respective pages.

4. Statistical test results

This RNG was previously certified and this is a recertification. There are minor changes in the certified code due to addition of Instant game. Diehard and Chisquare tests were not repeated. Additional Chisquare tests are performed for Instant game in this round of recertification. The following apply to previous testing rounds and addiotional tests for Instant game.

4.1 Testing results for raw output of RNG

The Diehard tests were performed on two random sequences. The columns 'Result Random sequence-1' and 'Result Random sequence-2' contain the filenames for the detailed results. These files are supplied as attachments with this Certification report.

Confidence Level for the tests is: 95%
Overall result: Pass

Result Random sequence-1	Result Random sequence-2	Sample size	Confidence level	Result
Refer to attachment Eyecon1.txt	Refer to attachment Eyecon2.txt	80 million bits	95%	Pass

4.2 Testing results for scaled/shuffled data

The Chi-square tests were performed with the results listed in Appendix A. The columns 'Result Datafile1' and 'Result Datafile 2' contain the filenames for the detailed results. These files are supplied with this Certification report.

Confidence Level for the tests is: 95%
Overall result: Pass

5. Final declaration and conformity

Nº	Description	Details
1.	Conditions/Observations	This RNG certification is restricted to Amazon Corretto Java runtime library version 8.0 to 22.x (Current version).
2.	Certification	Certification Date: 04 July 2024 Software Provider: Eyecon Alderney Limited Software Provider site URL: https://play.eyecongames.com/, https://play.eyeconalderney.gg Operator Name: N/A Operator site URL: N/A iTech Labs certifies that the Random Number Generator (RNG) as specified in Section 2.3 of this report and used by Eyecon Alderney Limited, complies with the Remote Technical and Operating Standards for the Gibraltar Gambling Industry - Gambling Commissioner's Guidelines - v.1.1.0. iTech Labs recommends that the Random Number Generator (RNG) specified in Section 2.3 of this report be approved for deployment, subject to the conditions listed in Section 5. Final declaration and conformity Item 1.

6. Conclusion

While it is not possible to test all possible scenarios in a laboratory environment, iTech Labs has conducted a level of testing appropriate for a submission of this type.

Accordingly, subject to the above comment, iTech Labs certifies that the items under test comply with the relevant Technical Standards, unless otherwise stated.

Signatures:

Divya Bhargava	
Divya Bhargava **Project Manager** **iTech Labs** 04 July 2024	**Alvin Rizaldi** **Chief Executive Officer** **iTech Labs** 04 July 2024

Appendix A – Chi Square Testing Result (refer to Section 4.2)

Table A.1 Non Card Games

Game Type	Range	DOF	Result Datafile 1 (Refer attachments)	Result Datafile2 (Refer attachments)	Scaled numbers*	C.L.^	Result
Slots	Weighted Single Number (5 elements, Sum of weights=120)	4	results-weighted1-20221021142614.xls	results-weighted1-20221021142915.xls	3400000	95%	Pass
	Weighted Single Number (12 elements, Sum of weights=3170)	11	results-weighted1-20221021142628.xls	results-weighted1-20221021142929.xls	3400000	95%	Pass
	Weighted Single Number (11 elements, Sum of weights=1000)	10	results-weighted1-20221021142636.xls	results-weighted1-20221021142937.xls	3400000	95%	Pass
	Weighted Single Number (12 elements, Sum of weights=39790)	11	results-weighted1-20221021142656.xls	results-weighted1-20221021142957.xls	10000000	95%	Pass
	Weighted Single Number (12 elements, Sum of weights=2613)	11	results-weighted1-20221021142712.xls	results-weighted1-20221021143641.xls	3400000	95%	Pass
	Weighted Single Number (5 elements, Sum of weights=100)	4	results-weighted1-20221021142730.xls	results-weighted1-20221021143031.xls	3400000	95%	Pass
	Weighted Single Number (8 elements, Sum of weights=1200)	7	results-weighted1-20221021142734.xls	results-weighted1-20221021143035.xls	3400000	95%	Pass
	29	28	single-29-results-20221021142704.xls	single-29-results-20221021143005.xls	4900000	95%	Pass
	30	29	single-30-results-20221021142718.xls	single-30-results-20221021143019.xls	4900000	95%	Pass
	32	31	single-32-results-20221021142618.xls	single-32-results-20221021142919.xls	4900000	95%	Pass
	33	32	single-33-results-20221021142728.xls	single-33-results-20221021143029.xls	4900000	95%	Pass
	34	33	single-34-results-20221021142714.xls	single-34-results-20221021143015.xls	4900000	95%	Pass
	35	34	single-35-results-20221021142634.xls	single-35-results-20221021142935.xls	4900000	95%	Pass
	36	35	single-36-results-20221021142708.xls	single-36-results-20221021143009.xls	4900000	95%	Pass
	37	36	single-37-results-20221021142654.xls	single-37-results-20221021142955.xls	4900000	95%	Pass
	38	37	single-38-results-20221021142716.xls	single-38-results-20221021143017.xls	4900000	95%	Pass
	39	38	single-39-results-20221021142720.xls	single-39-results-20221021143021.xls	4900000	95%	Pass
	40	39	single-40-results-20221021142638.xls	single-40-results-20221021143607.xls	4900000	95%	Pass
	41	40	single-41-results-20221021142622.xls	single-41-results-20221021142923.xls	4900000	95%	Pass
	42	41	single-42-results-20221021142632.xls	single-42-results-20221021142933.xls	4900000	95%	Pass
	43	42	single-43-results-20221021142724.xls	single-43-results-20221021143025.xls	4900000	95%	Pass
	44	43	single-44-results-20221021142706.xls	single-44-results-20221021143007.xls	4900000	95%	Pass
	45	44	single-45-results-20221021142732.xls	single-45-results-20221021143033.xls	4900000	95%	Pass
	46	45	single-46-results-20221021142650.xls	single-46-results-20221021142951.xls	4900000	95%	Pass

	48	47	single-48-results-20221021142710.xls	single-48-results-20221021143011.xls	4900000	95%	Pass
	49	48	single-49-results-20221021142646.xls	single-49-results-20221021142947.xls	4900000	95%	Pass
	52	51	single-52-results-20221021142722.xls	single-52-results-20221021143023.xls	4900000	95%	Pass
	57	56	single-57-results-20221021142702.xls	single-57-results-20221021143003.xls	4900000	95%	Pass
	59	58	single-59-results-20221021142640.xls	single-59-results-20221021142941.xls	4900000	95%	Pass
	60	59	single-60-results-20221021142624.xls	single-60-results-20221021142925.xls	4900000	95%	Pass
	64	63	single-64-results-20221021142652.xls	single-64-results-20221021142953.xls	4900000	95%	Pass
	67	66	single-67-results-20221021142648.xls	single-67-results-20221021142949.xls	4900000	95%	Pass
	68	67	single-68-results-20221021142630.xls	single-68-results-20221021142931.xls	4900000	95%	Pass
	69	68	single-69-results-20221021142616.xls	single-69-results-20221021142917.xls	4900000	95%	Pass
	71	70	single-71-results-20221021142644.xls	single-71-results-20221021142945.xls	4900000	95%	Pass
	72	71	single-72-results-20221021142700.xls	single-72-results-20221021143001.xls	4900000	95%	Pass
	73	72	single-73-results-20221021142612.xls	single-73-results-20221021142913.xls	4900000	95%	Pass
	75	74	single-75-results-20221021142726.xls	single-75-results-20221021143027.xls	4900000	95%	Pass
	76	75	single-76-results-20221021142736.xls	single-76-results-20221021143037.xls	4900000	95%	Pass
	78	77	single-78-results-20221021142620.xls	single-78-results-20221021142921.xls	4900000	95%	Pass
	80	79	single-80-results-20221021142626.xls	single-80-results-20221021142927.xls	4900000	95%	Pass
	88	87	single-88-results-20221021142642.xls	single-88-results-20221021142943.xls	4900000	95%	Pass
	90	89	single-90-results-20221021142610.xls	single-90-results-20221021142911.xls	4900000	95%	Pass
	93	92	single-93-results-20221021142658.xls	single-93-results-20221021142959.xls	4900000	95%	Pass
Instant	2	1	single-2-results-20240604135428.xls	single-2-results-20240604135524.xls	4900000	95%	Pass
	Weighted Single Number* (17 elements, Sum of weights=10145)	16	results-weighted1-20240604135442.xls	results-weighted1-20240604135538.xls	18000000	95%	Pass
	Weighted Single Number* (14 elements, Sum of weights=3946)	13	results-weighted2-20240604135430.xls	results-weighted2-20240604135526.xls	8500000	95%	Pass
	Weighted Single Number* (18 elements, Sum of weights=57883)	17	results-weighted3-20240605122500.xls	results-weighted3-20240605122738.xls	50000000	95%	Pass
	Weighted Single Number* (17 elements, Sum of weights=50383)	16	results-weighted4-20240605122506.xls	results-weighted4-20240605122745.xls	50000000	95%	Pass
	Weighted Single Number* (7 elements, Sum of weights=1032)	6	results-weighted5-20240604135432.xls	results-weighted5-20240604135528.xls	3400000	95%	Pass

** Scaled numbers for each data file; ^ Confidence Level*