

## **RGS EVALUATION TESTING REPORT**

### ***RNG – Random Number Generator***

#### **Reference regulation: Maltese Remote Gaming Regulations 2004**

(LEGAL NOTICE 176 of 2004, as amended by Legal Notices 110 of 2006,  
270 and 426 of 2007, 90 of 2011 and 131 of 2016.)

**29/09/2020**



## INTRODUCTION

The findings reported in this summary are the results of a broader set of documents and testing activities results archived in QUINEL Ltd's facilities. It is intended that the requester declares that:

- Any Hardware provided or described for analysis and testing is configured identically to hardware in commercial use
- Game software/ function provided for the testing and code review is declared by the customer to have the same behaviour to the software/code in commercial use
- Functionality made by the software in automatic test mode has a realistic behaviour

and that

- all the files and modules,
- the database schemas and all the specific programming resources,
- all the parameters contained into any databases and/or configuration file

that have been subject to the audit process guarantee the same behaviour of what is going to be published/deployed according to this audit results.

The Recipient, by accepting and using this Report, declares to be aware and accept unconditionally all the terms and conditions set forth. If the Applicant and / or the Recipient does not agree on the terms and conditions set forth, QUINEL Ltd reserves the right to cancel the certification provided with this Report, it follows therefore that the Recipient must immediately return all copies to QUINEL Ltd of this Report and cannot use them nor refer to.

Any copy of this test report must also include the page number and total number of pages.

Copy of this test report must not be reproduced except in full, without written approval of the laboratory.

**A) Audit ID**

J20091232\_R001\_RNG\_MT\_REV.1

**B) Reference regulation**

Maltese Remote Gaming Regulations 2004  
  
(LEGAL NOTICE 176 of 2004, as amended by Legal Notices 110 of 2006, 270 and 426 of 2007, 90 of 2011 and 131 of 2016.)

**C) Test methods**

QISI001– Software source code inspection  
 QIRT000 – RNG qualitative analysis  
 QIRT001 - Statistical analysis on scaled numbers in the range [0, 36] (Frequency, Couples, Serial Correlation and Run Tests)  
 QIRT002 - Statistical analysis on scaled numbers in the range [0, 51] (Frequency, Couples, Serial Correlation and Run Tests)  
 QIRT005 – DIEHARD battery of tests  
 QIRT006 – NIST battery of tests

**D) Auditor / Test lab (RGR Part VI, 26.b)**

**QUINEL Ltd**  
 M Space M3, Zone 3, Central Business District  
 Triq L-Ghajn tan-Nofs  
 Birkirkara CBD 3060 - Malta  
[info@quinel.com.mt](mailto:info@quinel.com.mt)

**E) Audit subject**

<b>Description:</b> Compliance of the following test items:			
<i>Test Item</i>	<i>Game Name</i>	<i>Version</i>	<i>Interface</i>
R001	RNG	1.0	N.A.
<b>Receipt date:</b> 10/03/2020 – first submission for testing against the regulation as per Section (B)			
<b>Inspection date:</b> 25/09/2020 - 29/09/2020			
<b>Note:</b> N.A.			

**F) Requester (RGR Part VI, 26.a)**

FUGASO Limited  
 Abacus Business Centre, Level 1 Triq Dun Karm, B'Kara Bypass  
 Birkirkara BKR 9037, Malta  
 info@fugaso.com

**G) Owner of the system/software (RGR Part VI, 26.a)**

Refer to section F)

**H) Companies and organizations involved in the process (RGR Part VI, 26.c)**

**Producer(s):** Ref. to Section G)

**Requester:** Ref. to Section F)

**Licensee/Operator:** N.A.

**I) Individuals involved in the process (RGR Part VI, 26.d)**

**On the Requester side:** Mr. Nikolai Mazger

**On the Producer(s) / Integrator(s) side:** same as for Requester.

**On the Licensee/Operator side:** N.A.

**J) Processes, rules and parameters of the games (RGR Part VI, 26.e)**

Evaluation of game rules was conducted to ensure that they satisfy the requirements as per the regulation in the Section (B). Refer to the Annex I for the full list of requirements satisfied.

Game / Test item type: **RNG - Random Number Generator**

Game(s) / Test item(s) use(s) Jackpot: N.A.

Here follows the theoretical pay-out of the test items:

<i>Test Item</i>	<i>Game/Item Name</i>	<i>Theor. RTP [%]</i>
R001	RNG	N.A.

**K) Protocols and specifications of the gaming system (RGR Part VI, 26.f)**

**Type:** software-based RNG

**Programming language:** Java

**Description of the RNG:**

The RNG is a wrapper for the Java *SecureRandom* library used to provide cryptographically strong random numbers. The *fugaso-rng-1.0.0.jar* library provides methods to extract both *Int32* and scaled number to the games.

**Security:**

SecureRandom algorithm is considered to be cryptographically secure.

For more details see: <https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html>.

All statistical tests have been performed by collecting sequences of scaled random numbers using a simulator, which is a utility to call the same methods that are used by the games to get necessary random numbers and save the result to file, provided by the Requester, deployed directly on the Requester's server.

Refer to the Annex I for the full list of requirements satisfied.

**L) Security of the system (RGR Part VI, 26.g)**

N.A.

**M) Critical modules (RGR Part VI, 26.h)**

<i>File name</i>	<i>SHA1</i>	<i>Description</i>	<i>Critical</i>	<i>Test Item</i>
fugaso-rng-1.0.0.jar	f57032abd267bb0873c31af7b1d13288f1b63281	RNG	Y	R001

**N) Evaluation performed**

The test evaluation, required by Requester (Ref. to Section F) was completed against the following requirements:

- *Third Schedule (Regulation 25)*

Refer to the Annex I for the full list of requirements satisfied.

**O) Testing activities applied**

Internal procedure followed: Rif. "IOP 02-02 TEST METHODS"

**P) Additional information (RGR Part VI, 26.i)**

None

**Q) Setup and application/system architecture (RGR Part VI, 26.j)**

Refer to Section K)

**R) Product Tested**

Refer to Section M)

**S) Report revisions**

N/A

**T) CERTIFICATION**

Date: 29/09/2020  
Requester: FUGASO Limited  
Abacus Business Centre, Level 1 Triq Dun Karm, B'Kara Bypass  
Birkirkara BKR 9037, Malta

Total Number of Pages: **10**

QUINEL Ltd certifies that the games / test items identified at section E) subject to testing and here briefly listed

R001: **RNG**

comply with the Remote Gaming Regulation of Malta (LEGAL NOTICE 176 of 2004, as amended by Legal Notices 110 of 2006, 270 and 426 of 2007, 90 of 2011 and 131 of 2016.).

Refer to the Annex I for the full list of requirements satisfied.

**U) CONDITIONS**

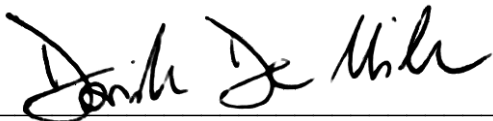
N.A.

**V) CONCLUSIONS**

QUINEL Ltd certifies that the RGS tested complies with the Technical Standards requested.

Date: 29/09/2020

**Signed:**



\_\_\_\_\_  
Davide De Nobile – Laboratory Manager  
(QUINEL Ltd)

## ANNEX I – REQUIREMENTS SATISFIED

DEFINITIONS
“ <b>the Act</b> ” means the Lotteries and Other Games Act, 2001
“ <b>appropriate resources</b> ” means financial resources which are, in the Authority’s sole discretion, adequate to ensure the financial viability of operations of a remote gaming office, and which are available from a source that is not tainted with illegality
“ <b>appropriate services</b> ” means the services of persons who have appropriate experience to ensure the proper and successful conduct of a remote gaming operation and, or a remote betting office
“ <b>approved control system</b> ” means a control system approved by the Authority, and shall include an approved control system changed or modified with the approval of the Authority
“ <b>authorised game</b> ” means remote gaming that a licensee is permitted to conduct under these regulation
“ <b>the Authority</b> ” means the Lotteries and Gaming Authority
“ <b>betting market</b> ” means a betting event with a well-defined termination point and decidable outcome
“ <b>control system</b> ” means a system of internal controls, and administrative and accounting procedures for the conduct of a remote gaming office which is set up and maintained in Malta
“ <b>electronic means</b> ” means all electronic data transfer, whether by telephone, facsimile, computer or any other means of distance communications as approved by the Authority
“ <b>game</b> ” has the same meaning assigned to it by the Act
“ <b>gaming</b> ” means an agreement, scheme, or arrangement between two or more parties to play together at a game of chance in which a prize or reward consisting of money or some other item of value, worth, advantage, or opportunity is offered or can be won and become the property of the winner under defined conditions established for the purpose of the game
“ <b>gaming records</b> ” means all records directly or indirectly related to remote gaming and to bets provided by a licensee and to player account information, wagers placed and to the outcomes of games played
“ <b>gaming system</b> ” means a computer system or systems of computers by means of which remote gaming is conducted, and shall include all its associated components, its operating systems and applications software
“ <b>inspector</b> ” has the same meaning assigned to it by article 17 of the Act
“ <b>key official</b> ” means a person nominated by the licensee who is a director of the licensee and resident in Malta
“ <b>licensee</b> ” means a person to whom the Authority has issued a remote gaming licence
“ <b>means of distance communications</b> ” has the same meaning assigned to it by the Act but shall not include press advertising with an order form or catalogue and phone-ins during radio and television programmes
“ <b>the Minister</b> ” means the Minister responsible for finance
“ <b>player</b> ” means any person who is over 18 years of age and who takes part in remote gaming
“ <b>player’s account</b> ” means a record kept by the licence holder, which record shall at all times be accessible to the player, which shows the player’s credit against such licence holder, taking into account all wagers placed and all prizes won by such player and any other debits or credits as may be permitted by these regulations or approved by the Authority
“ <b>pool betting</b> ” means betting made on terms where all or part of the winnings shall be determined by reference to the aggregate of stakes paid or agreed to be paid by the person betting, and which shall be divided among the winners
“ <b>remote betting</b> ” means the negotiation or receiving of any bet by a means of distance communications
“ <b>remote gaming</b> ” means any form of gaming by means of distance communications
“ <b>remote gaming equipment</b> ” means a machine or other device whether electronic, electrical or mechanical, computer software, or any other mechanism, device or item, used or suitable for use, in the operation of an authorised game and which is situated in Malta
“ <b>remote gaming licence</b> ” means the licence granted to a licensee by the Authority to conduct remote gaming
“ <b>remote gaming related activities</b> ” means any activity or business that the Authority considers reasonably related to the operation of remote gaming, or any business that offers goods or services to persons who

participate in licensed remote gaming
“ <b>qualifying shareholding</b> ” has the same meaning assigned to it by the Act
“ <b>stake</b> ” has the same meaning assigned to it by the Act.



Unless differently specified, the results are related to all the test items.

<b>Third Schedule</b>		
<b>Technical requirement for gaming system</b>		
1.	The gaming system must-	
(a)	faithfully follow the game rules published by the operator and	<i>N.A.</i>
(b)	provide over time no more than the expected house advantage to the operator	<i>N.A.</i>
2.	Both the gaming and financial transactions must be congruent and secure.	<i>N.A.</i>
3.	The gaming system must satisfy the following criteria for randomness, following Schneier-	
	(a) the data must be randomly generated, passing appropriate statistical tests of randomness.	<i>PASS</i>
	(b) the data must be unpredictable, i.e. it must be computationally infeasible to predict what the next number will be, given complete knowledge of the algorithm or hardware generating the sequence, and all previously generated numbers.	<i>PASS</i>
	(c) the series cannot be reliably reproduced, i.e. if the sequence generator is activated again with the same input (as exactly as is reasonably possible) it will produce two completely unrelated random sequences.	<i>PASS</i>
4.	The outcome of any game event, and the return to the player, must be independent of the CPU, memory, disk or other components used in the playing device used by the player	<i>N.A.</i>
5.	The game or any game event outcome must not be affected by the effective bandwidth, link utilisation, bit error rate or other characteristic of the communication channel between the gaming system and the playing device used by the player.	<i>N.A.</i>
6.	The gaming system must be able to display for each game the following information on the current page or on a page directly accessible from the current page via a hyperlink-	
	(a) the name of the game	<i>N.A.</i>
	(b) restrictions on play	<i>N.A.</i>
	(c) instructions on how to play, including a pay-table for all prizes and special features	<i>N.A.</i>
	(d) the player's current account balance	<i>N.A.</i>
	(e) unit and total bets	<i>N.A.</i>
	(f) the rules of the game	<i>N.A.</i>
	(g) information relating to the average winnings paid out to players of the game over a period of time or a particular number of plays	<i>N.A.</i>
7.	All financial reports produced by the gaming system must be congruent with gaming transaction reports and conversely	<i>N.A.</i>
	provided that all such reports shall be readily and freely available to the Authority	<i>N.A.</i>
8.	The gaming system must-	
	(a) be capable of producing monthly auditable and aggregate financial statements of gaming transactions, and	<i>N.A.</i>
	(b) calculate accurately all taxation and other monies due to the Authority	<i>N.A.</i>
9.	The gaming system must maintain information about all games played, including	
(a)	the identity of the player	<i>N.A.</i>
(b)	the time the game began as recorded on the games server	<i>N.A.</i>
(c)	the balance on the player's account at the start of the game	<i>N.A.</i>
(d)	the stakes placed in the game (time stamped by the games server)	<i>N.A.</i>
(e)	the game status (in progress, complete, etc	<i>N.A.</i>
(f)	the result of the game (time stamped by the games server)	<i>N.A.</i>

(g)	the time the game ended as recorded by the games server	N.A.
(h)	the amount won or lost by the player and	N.A.
(i)	the balance on the player's account at the end of the game	N.A.
10.	The gaming system must maintain information about significant events as follows-	
	(a) large wins	N.A.
	(b) transfers of funds in excess of such amount as the Authority may from time to time direct by notice in writing to the operator	N.A.
	(c) changes made by the operator to game parameters	N.A.
<i>11. Any variations to any of the requirements specified in this Schedule shall be submitted to the Authority for its approval by notice in writing.</i>		

<p>END OF COMPLIANCE REPORT</p>
---