RNG EVALUATION - TESTING REPORT

Reference regulations:

GLI-19 – Interactive Gaming Systems v2.0
(Chapter 4)

February 15th 2017

QUINEL M. Limited
Marina Court, Flat 8, Triq Giuseppe Cali', Ta'Xbiex – Malta
info@quinel.com.mt

TERMS AND CONDITIONS

The findings reported in this summary are the results of a broader set of documents and testing activities results archived in Quinel M's facilities. It is intended that the requester/manufacturer 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 behavior to the software/code in commercial use

- Functionality made by the software in automatic test mode has a realistic behavior and that

    o all the files and modules,

    o the database schemas and all the specific programming resources,

    o all the parameters contained into any databases and/or configuration file

that have been subject to the audit process guarantee the same behavior 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 reserves the right to cancel the certification provided with this Report, it follows therefore that the Recipient must immediately return all copies to Quinel of this Report and cannot use them nor refer to.

Any copy of this test reports and calibration certificates 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

BOO001RNG rev. 1

B) Reference Regulation(s)

GLI-19 – Interactive Gaming Systems v2.0 (Chapter 4)

C) Auditor / Test lab

Quinel M. Ltd Marina Court, Flat 8 Triq Giuseppe Cali' XBX1421 Ta'Xbiex - Malta VAT number MT 2115-0515

D) Audit subject

Description:

All statistical tests were performed by collecting random sequences of both raw and scaled numbers using an extraction tool provided by the customer and deployed on their machine.

All games use the same RNG instance on the application server. All games have access to the same RNG source since it is a wrapper for the O.S. /dev/urandom. therefore the background/cycling activity is implied in the usage of the same RNG source by different games.

The RNG uses different entropy sources:

"The random number generator gathers environmental noise from device drivers and other sources into an entropy pool. The generator also keeps an estimate of the number of bits of noise in the entropy pool. From this entropy pool random numbers are created."
(From https://linux.die.net/man/4/urandom)

The core files analyzed in the audit are:

sources.py ca113d9f657d325358cc169903e346d9da2d5e01	CRITICAL - Core script of the RNG extractor
algorithms.py 16a7f79b204a242c6b1de9d86e45642b687852bb	CRITICAL - Script to manage the mapping methods
platform.tar.gz a3c5b286a5ccb3dff1091bc829bd153933fb859e	Core platform files, including the abovementioned sources.py, used to deliver the RNG data to the application
jklib.tar.gz 6d0eeb3e4a032e1a0265ea242a52ad89fd0b5aef	Core application library files, including the abovementioned algorithm.py, used to get the RNG from the platform

E) Receipt date

January 17th 2017

F) Testing period:

Jan 17th, 2017 – Feb 14th, 2017

G) Requester / Manufacturer

BOOONGO ENTERTAINMENT N.V

E-Commerce Park Vredenberg,

Curaçao

H) Companies and organizations involved in the process

Requester/producer:

BOOONGO ENTERTAINMENT N.V

E-Commerce Park Vredenberg

Curaçao

I) Individuals involved in the process

On the Requester/Manufacturer side:

Anton Horunov – Backend development Team Lead

Nika Krupitskaya – Project Manager

J) Processes, rules and parameters of the games

-

K) Evaluation performed

The test evaluation of software, as required by BOOONGO ENTERTAINMENT N.V. was completed against the following requirements:

- *GLI-19 Standard, Chapter 4*

The list of the requirements included into the testing scope required by BOOONGO ENTERTAINMENT N.V their applicability and the compliance outcomes are listed into the detailed ANNEX REPORT.

L) Additional information

The RNG is integrated with games and, it was verified by means of a supervised session, that it is deployed in production environment.

M) CERTIFICATION

Date: **February 15th 2017**

Requester/Manufacturer: **BOOONGO ENTERTAINMENT N.V**
                               E-Commerce Park Vredenberg
                               Curaçao

Total Number of Pages: **8**

QUINEL M. certifies that the test items examined comply with

-   *The GLI-19 – Interactive Gaming Systems v2.0 (Chapter 4) standard*

Refer to the annex report for the full list of requirement satisfied.

N) CONDITIONS

Validity of this report is bound to the fulfillment of the conditions reported into the Terms and Conditions.

Date: February 15th, 2017
Signed:

_____
Matteo Ferrarini - COO (QUINEL M LTD)

ANNEX REPORT

REGULATION: GLI-19 – Interactive Gaming Systems v2.0 (Chapter 4)

4.1 Introduction	Result	Notes
4.1.1 General Statement. The random number generator must be cryptographically strong at the time of submission. Where more than one instance of a random number generator is used in an Interactive Gaming System, each instance must be separately evaluated and certified. Where each instance is identical, but involves a different implementation within game(s) / application(s), each implementation must also be separately evaluated and certified. Any outcomes from the random number generator used for game symbol selection / game outcome determination must be shown, via data analysis and a source code read, to:	PASS	
a) Be statistically independent	PASS	
b) Be fairly distributed (within statistically expected bounds) over their range	PASS	
c) Pass various recognized statistical tests	PASS	
d) Be cryptographically strong	PASS	
4.1.2 Applied Tests. The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to: a) Chi-square test; b) Equi-distribution (frequency) test; c) Gap test; d) Overlaps test; e) Poker test; f) Coupon collector's test;	PASS	

4.1 Introduction	Result	Notes

g) Permutation test;
   h) Kolmogorov-Smirnov test;
   i) Adjacency criterion tests;
   j) Order statistic test;
   k) Runs tests (patterns of occurrences should not be recurrent);
   l) Interplay correlation test;
   m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);
   n) Tests on subsequences; and
   o) Poisson distribution.		

4.2 Scaling	Result	Notes
4.2.1 General Statement. The scaling method shall not compromise the cryptographic strength of the random number generator. Additionally, the scaling method shall preserve the distribution of the scaled values. For example, if a 32-bit random number generator with a range of the set of integers in the closed interval $[0, 2^{32} - 1]$ were to be scaled to the range of set the of integers in the closed interval $[1,6]$ so that the scaled values can be used to simulate the roll of a standard sixsided die, then each integer in the scaled range should theoretically appear with equal frequency. In the example given, if the theoretical frequency for each value is not equal, then the scaling method is considered to have a bias. Thus, a compliant scaling method shall have bias equal to zero.	PASS	

4.3 Hardware-Based RNG	Result	Notes
4.3.1 General Statement. Owing to their physical nature, the performance of hardware-based RNGs can deteriorate over time. The failure of a hardware-based RNG could have serious consequences for the game(s) / application(s), as games may become predictable or exhibit nonfair distribution. Accordingly, if a hardware-based RNG is used, there must be dynamic / active, real-time monitoring of the output with a sample size large enough to allow for reasonably high statistically powerful testing, such that game play is disabled when an output	NA	The RNG is not Hardware Based

4.3 Hardware-Based RNG	Result	Notes
testing failure is detected.		

4.4 Software-Based RNG	Result	Notes
4.4.1 General Statement. The following requirements apply only to software-based RNGs.	-	
4.4.2 Period. The period of the RNG, in conjunction with the methods of implementing the RNG outcomes, must be sufficiently large to ensure that all game independent outcome combinations / permutations are possible for the given game(s) / application(s).	PASS	
4.4.3 Seeding/Re-Seeding. The methods of seeding / re-seeding must ensure that all seed values are determined in a manner that does not compromise the cryptographic security of the random number generator.	PASS	
4.4.4 Background Cycling/Activity. In order to ensure that RNG outcomes cannot be predicted, adequate background cycling / activity must be implemented in between games. Wherever a game outcome is made up of multiple mapped RNG values, background cycling / activity must be implemented during the game (i.e.: in between the selection of each mapped RNG value) in order to ensure that the game outcome is not comprised of sequential mapped RNG outcomes. The rate of background cycling / activity must be sufficiently random in and of itself to prevent prediction.	PASS	

END
OF
DOCUMENT