RNG EVALUATION TESTING REPORT

Reference regulations:

GLI-19 – Interactive Gaming Systems v2.0

20/06/2019

QUINEL Limited
Marina Court, Flat 8 Triq Giuseppe Calì
XBX1421 Ta' Xbiex - Malta
info@quinel.com.mt

INTRODUCTION

The findings reported in this summary are the results of a broader set of documents and testing activities results archived in QUINEL Limited'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.

A) Audit ID

CRY001GAM

B) Reference Regulation(s)

GLI-19 – Interactive Gaming Systems v2.0

C) Auditor / Test lab

QUINEL Limited
Marina Court, Flat 8 Triq Giuseppe Calì
XBX1421 Ta' Xbiex - Malta

D) Audit subject

Description:
Compliance of the following test items (games):

Test Item	*Item Name*	*Version*	*Interface*
R001	**RNG**	**1.0**	**N.A.**

Receipt date:
08/10/2018

Test date:
24/01/2019 - 18/06/2019

E) Requester / Licensee / Producer

CRYSTALNET LIMITED
8 Copthall, Roseau Valley,
00152, Commonwealth of Dominica

F) Companies and organizations involved in the process

Refer to section E)

G) Individuals involved in the process

Pavel Fedyushin - CBDO
Maksym Roienko - CTO
Sergii Busygin - Delivery Manager

H) Processes, rules and parameters of the games

Evaluation of game rules (if test item is a game) 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**
Game / Test item use Jackpot: **No**
Here follows the theoretical pay-out of the test item(s):

Test Item	*Test Item / Game name*	*Theor. RTP [%]*
R001	**RNG**	**N.A.**

I) Protocols and specifications of the gaming system

Programming language: C++
Architecture:
The requestor has created an interface that uses the "uniform_int_distribution" class from C++ for generates cryptographically secure pseudo-random integers. In order to ensure more security and unpredictability a background cycle continuosly drops a random amount of extraction from the RNG.
Reseeding:
Every day the RNG is reset using random data from the integrated Linux "/dev/urandom" feature.
More information:
- https://linux.die.net/man/4/urandom
- https://en.cppreference.com/w/cpp/numeric/random/uniform_int_distribution
Usage:
All games call the unique instance of the RNG core binaries and must use it as is without any manipulations.
Tested strings:
The tests were performed against those functions able to extract:
- 32-bit integers
- Integer number scaled within specific ranges used within the test items:
  [0-36]
  [0-51]
- 32-bit floating-point number in range [0,1) with 8-digit precision

J) Security of the system

N.A.

K) Evaluation performed

The test evaluation, required by the Requester, was completed against the "GLI-19 – Interactive Gaming Systems v2.0"

Refer to the Annex I for a full detailed list of requirements tested.

L) Additional information

N.A.

M) Product Tested and critical files

The tests were performed on the files listed below:

File name	*SHA1*	*Description*	*Critical*	*Test Item*
seedupdater	28cce53d96858f967b0d15cfbdab32ead5b3d825	RNG	Y	**R001**
rngenerator	9b7544a767846c17fc85865f56a3101af41085d3	RNG	Y	**R001**

N) CERTIFICATION

Requester / Licensee / Producer:
CRYSTALNET LIMITED
8 Copthall, Roseau Valley,
00152, Commonwealth of Dominica

Total Number of Pages: **8**

QUINEL Limited certifies that the test items examined comply with the requirement listed in the Annex I of the following regulations:

- the *GLI-19 – Interactive Gaming Systems v2.0 standard*

O) CONDITIONS

None

P) CONCLUSIONS

The games / test items identified at section D) are compliant with the abovementioned technical standards.

Date: 20/06/2019

Signed:

Davide De Nobile – Laboratory Manager
QUINEL Limited

ANNEX I

REGULATION: GLI-19 – Interactive Gaming Systems v2.0

CHAPTER 4 - Random number generator (RNG) requirements

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; and	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:	PASS	
e) Chi-square test;	PASS	
f) Equi-distribution (frequency) test;	PASS	
g) Gap test;	PASS	
h) Overlaps test;	PASS	
i) Poker test;	PASS	
j) Coupon collector's test;	N/A	
k) Permutation test;	N/A	
l) Kolmogorov-Smirnov test;	N/A	

m) Adjacency criterion tests;	PASS	
n) Order statistic test;	PASS	
o) Runs tests (patterns of occurrences should not be recurrent);	PASS	
p) Interplay correlation test;	PASS	
q) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);	PASS	
r) Tests on subsequences; and	PASS	
s) Poisson distribution.	N/A	

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, 232-1] 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 testing failure is detected.	N/A	Software RNG

4.4 Software-Based RNG	Result	Notes
4.4.1 General Statement. The following requirements apply only to software-based RNGs.	PASS	
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
COMPLIANCE
REPORT

QUINEL Limited
Marina Court, Flat 8 Triq Giuseppe Calì
XBX1421 Ta' Xbiex - Malta
info@quinel.com.mt