RANDOM NUMBER GENERATOR EVALUATION

TESTING REPORT

RNG revision 3.5.0

Reference regulation: Estonian Gambling Act – Riigi Teataja

(Passed 15.10.2008
RT I 2008, 47, 261
Entry into force 01.01.2009, partly the date of entry into force pursuant to § 111
Published on 01.01.2016, English translation published on 15.01.2016)

Organisation of Remote Gambling

March 25th, 2016

QUINEL M Limited
Marina Court, Flat 8, Triq Giuseppe Cali', XBX 1421 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 M'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

J16030078_RNG_Vers. 3.5.0_rev. 1

B) Reference regulation

Reference regulation: Estonian Gambling Act – Riigi Teataja
(Passed 15.10.2008; RT I 2008, 47, 261;
Entry into force 01.01.2009, partly the date of entry into force pursuant to § 111
Published on 01.01.2016, English translation published on 15.01.2016)
Organisation of Remote Gambling

C) Test methods

QISI001– Software source code inspection
QIRT000 – RNG qualitative analysis
QIRT001 (UD01 / SI01 / RT01) - Uniform distribution , statistical independence, Runs tests
ERT001 – DIEHARD battery of tests
ERT002 – NIST (SP800-22rev1a) battery of tests
QIRT002 (SS01) – Statistical analysis on scaled/mapped/shuffled numbers (Gap test, Serial test, etc)

All tests regarding the RNG were performed using
RNGTesterApp.exe – version 1.3.3

D) Auditor / Test lab

Quinel M. LTD
Marina Court, Flat 8,
Triq Giuseppe Cali',
XBX 1421 Ta'Xbiex - Malta
info@quinel.com.mt

E) Audit subject / Scope

Description:
Compliance testing of RNG

Test Items

Test Item	*Game/Item Name*	*Revision*	*Interface*
R001	RNG	3.5.0	N/A

Receipt date:
- 22/03/2016 – first submission for testing against current regulation

Inspection date:
- 22/03/2016 - 25/03/2016 (against current regulation)

F) Requester

Thunderkick Malta LTD
Level 5, The Mall Complex,
Floriana, Malta

G) Owner/Producer of the system/software

Ref. to Section F)

H) Companies and organizations involved in the process

Producer(s): Ref. to Section G)

Requester: Ref. to Section F)

Licensee/Operator: Ref. to Section F)

I) Individuals involved in the process

On the Requester side: Mr. Sven Grip, Mr. Stéphane Redon, Mr. Johnny Aspelin, Mr. Daniel Gjörwell, Ms. Jeanette Karlsson.

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

On the Licensee/Operator side: same as for Requester

J) Processes, rules and parameters of the games / Limitation of use

Random number generator
Type: software-based RNG
Test results are reported with details into Annex II.

Programming Language: Java
Algorithm: *Mersenne Twister*

Architecture
A unique instance of *Mersenne Twister* is shared among the games.

Usage
All games call the unique instance of the RNG core binaries and must use it as is without any manipulations.

K) Protocols and specifications of the gaming system

N.A.

L) File analysed / Critical modules

Refer to the following table

Configurations: refer to section J for those found and evaluated.

Relevant binaries:

SHA1	*Critical*	*Type*	*Test item*	*Filen ame*
f2dcd4e8ed46eb5653d99ff54f60c4e4047ad4ec	Yes	Game logic	R001	rng-implementation\gp-rng-3.5.0-RELEASE.jar
ea01386be069745202580bd50c3de32c33f3553f	Yes	Game logic	R001	rng-interface\gp-rng-api-3.5.0-RELEASE.jar

Sources:

SHA1	*Critical*	*Type*	*Test item*	*Filename*
d5e01a5f41deae3b63b46b2ccb7125278e3ebc29	Yes	Game logic	R001	gp-rng\...\MersenneTwister32.java
ea8940a1cd7d561eb944c42f101ddfcd7cce2ec7	Yes	Game logic	R001	gp-rng-api\...\RandomNumberGenerator.java
726a2f16d4bb551891fc2d70fd51e5f7880b2073	No	runtime check process	R001	gp-rng-test\...\DistributionVisualization.java
72c75a15b319929b58caf2c1ee7640da56a89c4e	No	runtime check process	R001	gp-rng-test\...\MersenneTwister32Data.java
16a7236b3cdb4c790c9d2f5799e0d5ccc7db2e38	No	runtime check process	R001	gp-rng-test\...\MersenneTwister32Test.java

M)Evaluation performed

The test evaluation, required by the Requested, was completed against the "*Remote gambling and software technical standard"* to meet Level 1 compliance as per the "*Testing strategy for compliance with remote gambling and software technical standards*", July 2015

RNG:
Tests were performed against those functions able to extract:
- Raw 32 bit integers
- scaled numbers in the intervals:
[0,36]
[0,51]
[0,99]
[0,149]
[0,199]
[0,249]

Refer to the Annex I for a full detailed list of requirements tested.
Refer to the Annex II for a full detailed list of details related to RNG testing.

N) Testing activities applied

- Randomness of the RNG
- Source code inspection

O) Additional information

None

P) Product Tested

Refer to section L)

Q) CERTIFICATION

Date: March 25th, 2016 Job: J16030078
Requester: Thunderkick Malta LTD
Level 5, The Mall Complex,
Floriana, Malta

Total Number of Pages: **12**

QUINEL M. LTD certifies that the test items examined comply with the Reference regulation: Estonian Gambling Act – Riigi Teataja
(Passed 15.10.2008; RT I 2008, 47, 261; Entry into force 01.01.2009, partly the date of entry into force pursuant to § 111; Published on 01.01.2016, English translation published on 15.01.2016)
Organisation of Remote Gambling

Test item(s):
- R001: RNG, vers. 3.5.0

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

R) CONDITIONS

None.

S) CONCLUSIONS

QUINEL M LTD certifies that the RNG tested complies with the Technical Standards requested.

Date: March 25th, 2016
Signed:

Matteo Ferrarini – Laboratory Technical Director
Chief Operation Officer (QUINEL M)

ANNEX I – REQUIREMENTS SATISFIED

Since the Estonian Guidelines do not provide any requirement regarding RNG testing and certification except that: "*The assessment of the independent expert must assure inter alia that the software used for organisation of gambling as remote gambling shall include the random number generator (RNG) for determining winnings.*", Quinel M. LTD reports that the RNG certified meets the requirements of most European regulated jurisdictions (e.g.:

Malta - Maltese Remote Gaming Regulations 2004 (Legal Notice 176 of 2004 of the Lotteries and other Games Act - ACT XXIV OF 2001 and further amendments by Legal Notices 110 of 2006, 270 and 426 of 2007, and 90 of 2011)

United Kingdom - UK Gambling Commission - Remote gambling and software technical standards, July 2015)

ANNEX II – RNG test details

A) Security

RNG output is used immediately and not stored in memory. Restarting of RNG is not performed programmatically and requires the entire platform to restart. Background cycling is in fact implemented sharing the RNG instance among all the games.

B) Testing results for raw output of RNG (section 3.6.1)

Data extraction scripts:

```
bffc82e40fd4e17cc8b0a3573ddeaa58ce60755d *Estrattore.zip
```

Data sets (3 million outcomes each, raw 32 bit integers):

```
be07ad3a58bca9bdbca5649a3c17547c755e51ae *raw_3M_1.txt
e4a6dbd88036613365e575aca890f4f76b280eff *raw_3M_2.txt
34fdf1b14d37739cdd485e65bc86c0dac6c141ac *raw_3M_3.txt
```

DIEHARD battery of tests

Overall results: POSITIVE

Test results:

BIRTHDAY SPACINGS TEST:	PASS
OVERLAPPING 5-PERMUTATION TEST:	PASS
BINARY RANK TEST for 31x31M:	PASS
BINARY RANK TEST for 32x32M:	PASS
BINARY RANK TEST for 6x8M:	PASS
BITSTREAM TEST:	PASS
OPSO, OQSO and DNA TESTS:	PASS
COUNT-THE-1's TEST (stream) :	PASS
COUNT-THE-1's TEST (specific) :	PASS
PARKING LOT TEST:	PASS
MINIMUM DISTANCE TEST:	PASS
3DSPHERES TEST:	PASS
SQEEZE TEST:	PASS
OVERLAPPING SUMS TEST:	PASS
RUNS TEST:	PASS
CRAPS TEST:	PASS

NIST battery of tests:

Overall results: POSITIVE

Test results:

Frequency:	PASS
BlockFrequency:	PASS
CumulativeSums:	PASS
Runs:	PASS
LongestRun:	PASS
Rank:	PASS
FFT:	PASS
NonOverlappingTemplate:	PASS
OverlappingTemplate:	PASS
Universal:	PASS
ApproximateEntropy:	PASS
RandomExcursions:	PASS
RandomExcursionsVariant:	PASS
Serial:	PASS
LinearComplexity:	PASS

C) Testing results for scaled data or shuffled decks data (section 3.6.2)

Data extraction scripts:

```
bffc82e40fd4e17cc8b0a3573ddeaa58ce60755d *Estrattore.zip
```

Confidence level: 95%

1) Data sets (3 million outcomes each, random extraction DOF = 36, range=[0,36] (included)):

```
7fed3b9d4464136e6a90556883ce623ac52f25e6 *36_300K_0.txt
5d85d7a11d366be2a0ba277f5279c9214adafee7 *36_300K_1.txt
0dbd067eb8b773622616c935732e1ad5c3be2f76 *36_300K_2.txt
ccae19f4104bfae3f44775677de42c013d02609c *36_300K_3.txt
f56c2c4ea06927198f9008ca6c7b8919ac34aa2c *36_300K_4.txt
298f594018645dd455f32d5de1d3277263984b62 *36_300K_5.txt
12441be957fa3f9b1e77a9b8e40d6429b4097c36 *36_300K_6.txt
24f27ea7f9332cd85b5707e9c4753bd794f157da *36_300K_7.txt
ceaa227b1b295929d1095d6f7794161baa67b31c *36_300K_8.txt
3fb5700e8dec2b2bb50b3ecf9a6a268c43ebaee4 *36_300K_9.txt
164b92581eea874ee881b0fe93db1f40403e3569 *36_3M_0.txt
8cf358def90e611f1a13666ca54eb71929255662 *36_3M_1.txt
05c8ae5ecb0a7a4d8bb3b1290d41f87ab0015546 *36_3M_2.txt
```

2) Data sets (3 million outcomes each, random extraction DOF = 52, range=[0,51] (included)):

```
1470056e451ee7a84e8df28ca1205419bc9cd58e *52_300K_0.txt
071ce958cd2ae553f8b0875b461c03bc673dbec8 *52_300K_1.txt
b21492ec2c1fd4eab438cca3362a16215c083da4 *52_300K_2.txt
229be47b788ac17dc6e90b95202d3bf1b8ed3094 *52_300K_3.txt
cd82b98355a92b3075f8a91317230ad5db4ec10c *52_300K_4.txt
562403c39d7436cbe850cffc9bf4c3434dee8d78 *52_300K_5.txt
```

```
f89e8acd6f75e33a0469a658b6ec6a917b2f2936 *52_300K_6.txt
8b3c8c5b4189f0a6af80b6086c64b4198b15a65e *52_300K_7.txt
3c32f8281d85a12f74f05fc546350bb3e1bdadee *52_300K_8.txt
2748ce90b0160fdf9b44b9379eb4999e5defe147 *52_300K_9.txt
4c46c9560d0138b95853c9605bfec229736a29d7 *52_3M_0.txt
2f32b79eac29710633c4e143cd7901da98e6f1dd *52_3M_1.txt
9143b59accec4ce927b7b0ec5115e387db6562bc *52_3M_2.txt
```

3) Data sets (3 million outcomes each, random extraction DOF = 100, range=[0,99] (included)):

```
ba3028a649f64da3e89c25585d293ab9e102e1df *100_300K_0.txt
a900151ba7695cc859d68a293ee0db3d0883b8b0 *100_300K_1.txt
b37af1340951e7ab1ca1bba658dab07324b09973 *100_300K_2.txt
d24195f1814ad766f5f838aed70517cc1f993931 *100_300K_3.txt
8c0ff73793a4e9a311e965ea8c848de413d439df *100_300K_4.txt
6c9bd752f972cf4d14de1e54d7a843591de2c3e1 *100_300K_5.txt
0b8e438f1225a0ecf287b2a0adb0fe1f3e7e166c *100_300K_6.txt
c56bc67bb0bb102d7c9372e0d371b6b5c16ddde7 *100_300K_7.txt
993ccb67774d1246e1d3cf2a7ee988ea0d126e04 *100_300K_8.txt
20b6a7651b3d0e2d67258089763a8024885bd798 *100_300K_9.txt
d8aa52bca9395a9754a22f3e5eb2a20e1ed865b7 *100_3M_0.txt
19a7eb7485a863efb24f1d9573ffeff9039300b4 *100_3M_1.txt
7a0d222698b5b42ed5163d4fde23bc95912a413e *100_3M_2.txt
```

4) Data sets (3 million outcomes each, random extraction DOF = 150, range=[0,149] (included)):

```
1009c9b23c265506829a010b708f32267a794a56 *150_300K_0.txt
ffde58f97c39f34425c1534882722b04bddd4efe *150_300K_1.txt
5b9313b95481e49db570e7e4bc38cf5233834c1b *150_300K_2.txt
95417d795b2bf3011250318473bd9476dbf8bbdf *150_300K_3.txt
0a7dab99c7682b21293430ba65ad6eab150b0106 *150_300K_4.txt
dbb5b147a69e07a418e20d85c19a9689c7371981 *150_300K_5.txt
3f0ff84f22b3aba3f97cf1d6667ff7cfaa714928 *150_300K_6.txt
3e997f5a9d78bbc03c08f5f108317ba3ce993345 *150_300K_7.txt
71415599e1d2a00d2b466ef3275de5ff9ec59089 *150_300K_8.txt
09f9d091fa39d3abb950a17ffc655fb0a74be18f *150_300K_9.txt
9397e8729c38b4e8fb14eab2a66741a9c4850ee4 *150_3M_0.txt
8a12e3ed07537303ecc72688d68fb3e30ca451a5 *150_3M_1.txt
25d7a754219112ff1544a3f234c21896805cfd7a *150_3M_2.txt
```

5) Data sets (3 million outcomes each, random extraction DOF = 200, range=[0,199] (included)):

```
4e289ef150205676708194c5871f16e162ee1182 *200_300K_0.txt
c264ed2030420012e4a1a01578fafe62276af0d7 *200_300K_1.txt
01444e0c1a16eb249c613582ba0c3548192f4e86 *200_300K_2.txt
d887073aefc42c9d92e0a2edeeb80de4adb091f0 *200_300K_3.txt
1251f0fee2b584edb8584efd9bc0a031c32eb0bc *200_300K_4.txt
d50368ce7c448a0d824f66d5e4817bdf24b6f7be *200_300K_5.txt
8d34d6c69bcdca9d195fb386f8bbd75a86e8e1a6 *200_300K_6.txt
f3eb9c9a2b71d86733ad87eeb5e7227dcf75549f *200_300K_7.txt
52368eb9b3776d636ec5329012719cad2aa69a02 *200_300K_8.txt
a91ab0f70e2692a92313fd63e1d9bbdd8b171957 *200_300K_9.txt
```

```
16a5821ba6874b39119f36833fee23a3c2e4423e *200_3M_0.txt
2eee04dcfb9c9405227f0161badecc4b131965eb *200_3M_1.txt
7d9b912698166c72aa7c93deb03263939d9ea27b *200_3M_2.txt
```

6) Data sets (3 million outcomes each, random extraction DOF = 250, range=[0,249] (included)):

```
a33b791c01d91045ee8c6e17bc7981af1f7954be *250_300K_0.txt
d1f11c42553527ab7671437a4839561b6eb68e73 *250_300K_1.txt
c25e476d8f1f71e3004cc6ff068643aefa20c0cf *250_300K_2.txt
dd9865baea59ea500d9faac9868f6565d1098a9e *250_300K_3.txt
566df8c7b3ad0ec90a15c6993a137576529f99f0 *250_300K_4.txt
2c4917c595760e2c08912da0fa6e96ab604d8c32 *250_300K_5.txt
3b326ef8100d2e3540ec50a85728bc751400a76e *250_300K_6.txt
bdb3a57fb9a69760f92db54b0f9b0a881bc04c67 *250_300K_7.txt
40a793795287431448f73bcc636ba44d5512bcfc *250_300K_8.txt
d8570904f8f4f6e79be026af31bc2893b89e3170 *250_300K_9.txt
4cfb3f90aa771333398a893464a4ef235003775f *250_3M_0.txt
0fc0fdd0a8446cdcbdf2cf6fae127ef3b7ec672a *250_3M_1.txt
28cb8ca81637c7a80beae9026066d41235270499 *250_3M_2.txt
```

Overall results: POSITIVE

Test results:

UNIFORM DISTRIBUTION / FREQUENCY:	PASS
STATISTICAL INDEPENDENCE (Chi square):	PASS
RUNS TESTS:	PASS
SELF-CORRELATION:	PASS
CROSS-CORRELATION:	PASS

END
OF
COMPLIANCE
REPORT