

JOGOS REMOTOS

RELATÓRIO DO TESTE DE AVALIAÇÃO

RNG:

ORTIZ

Regulamento de referência:
LOTTOPAR (Loterias do Estado do Paraná) - Regulamentação de jogos on-line

11/11/2024

INTRODUÇÃO

As conclusões apresentadas neste resumo são o resultado de um conjunto mais vasto de documentos e resultados de atividades de teste arquivados nas instalações da QUINEL Ltd. Pretende-se que o requerente declare que:

- Qualquer hardware fornecido ou descrito para análise e teste está configurado de forma idêntica ao hardware em uso comercial
- O software/função de jogo fornecido para a testagem e revisão de código é declarado pelo cliente como tendo o mesmo comportamento que o software/código em uso comercial
- A funcionalidade criada pelo software em modo de teste automático tem um comportamento realista

e que

- todos os ficheiros e módulos,
- os esquemas das bases de dados e todos os recursos específicos de programação,
- todos os parâmetros contidos em qualquer base de dados e/ou ficheiro de configuração

que foram sujeitos ao processo de auditoria garantem o mesmo comportamento do que vai ser publicado/implantado de acordo com os resultados desta auditoria.

O Destinatário, ao aceitar e utilizar este Relatório, declara estar ciente e aceitar incondicionalmente todos os termos e condições estabelecidos. Se o Requerente e / ou o Destinatário não concordar com os termos e condições estabelecidos, a QUINEL Ltd. reserva-se o direito de cancelar a certificação fornecida com este Relatório, o que implica que o Destinatário deverá devolver imediatamente todas as cópias deste Relatório à Quinel Ltd. e não poderá utilizá-las.

Qualquer cópia deste relatório de conformidade deve também incluir o número da página e o número total de páginas.

A cópia deste relatório de teste não pode ser reproduzida exceto na íntegra, sem a aprovação por escrito do laboratório.

QUINEL Ltd

M Space M3 – Zone 3, Central Business District Triq L-Ghajj tan – Nofs – Birkirkara CBD 3060- Malta

info@quinel.com.mt

A) ID do relatório

BR-PR_ORT001RNG.1_REV.1

B) Regulamento de referência

PORTARIA N° 079/2024 – LOTTOPAR
PORTARIA N° 080/2024 – LOTTOPAR
GLI-19 - Standards for *Interactive Gaming Systems* - v3.0

C) Métodos de teste

QISI001 - Método de inspeção do código-fonte de software
QIRT000 - Análise qualitativa RNG
QIRT001 - Análise estatística de números escalonados na faixa [0, 36]
QIRT002 - Análise estatística de números escalonados na faixa [0, 51]
QIRT003 - Análise estatística de números flutuantes na faixa [0, 1)
QIRT004 - Análise estatística de números baralhados
QIRT005 - Bateria de testes DIEHARD
QIRT006 - Bateria de testes NIST

D) Laboratório de emissão

QUINEL Ltd
M Space M3, Zone 3, Central Business District
Triq L-Ghajj tan- Nofs
Birkirkara CBD 3060- Malta
info@quinel.com.mt

E) Escopo

Descrição: Conformidade dos seguinte(s) item(ns) de teste:

Item de Teste	Nome do item	Versão	Interface
R001	RNG Software	1.2.0	N.A.

Data de recebimento:

15/08/2024 – primeiro envio para teste conforme o regulamento da Secção (B)

Data da avaliação:

23/09/2024 - 11/11/2024

F) Requerente

ORTIZ GAMING, S.L.
Calle Pollensa (Ed. Artemisa), 2 – Oficina 25 28290

Las Rozas de Madrid, Madrid, (Spain)
compliance@ortizgaming.com

G) Proprietário/Produtor do sistema/software

Consulte a secção F)

H) Empresas e organizações envolvidas no processo

Produtor(es): Cons. à Secção G)

Requerente: Cons. à Secção F)

Titular da licença/Operador: N.A.

I) Indivíduos envolvidos no processo

Do lado do Requerente: Mauricio Tadeu Alegretti - Chief Technology Officer

Do lado do(s) Produtor(es) / Integrador(es): o mesmo que para o Requerente

Do lado do Titular da licença/Operador: N.A.

J) Informações sobre os itens

Tipo de jogo /item de teste: **Gerador de Números Aleatórios**

Jogo /Item de teste usa Jackpot: **N.A.**

Segue o pagamento teórico do(s) item(ns) de teste:

<i>Item de Teste</i>	<i>Item de teste/Nome do jogo</i>	<i>Teor. RTP [%]</i>
R001	RNG Software	N.A.

K) Especificações do sistema de jogo

Tipo: RNG baseado em software

Linguagem de programação: C++

Kernel do Linux: 6.5.0

Descrição do RNG:

O RNG é escrito inteiramente com C++ e usa Nginx como proxy reverso.

A função *getNext()* gera inteiros cobrindo o intervalo de 32 bits. O servidor RNG consiste em dois pacotes: *rng-server* e *libfortuna*. *rng-server* é responsável por lidar com as solicitações e as respostas ao *libfortuna*, que implementa um algoritmo Fortuna de acordo com a implementação pública.

Segurança:

O algoritmo é baseado no algoritmo Fortuna, que é criptograficamente forte

QUINEL Ltd

M Space M3 – Zone 3, Central Business District Triq L-Ghajj tan – Nofs – Birkirkara CBD 3060- Malta

info@quinel.com.mt

Veja: <https://www.schneier.com/academic/fortuna/>

Consulte o Anexo II para uma lista detalhada cheia de detalhes relacionados a testes de RNG.

L) Módulos críticos

Consulte a secção Q)

M) Avaliação realizada

A avaliação do teste, exigida pelo Requerente, foi concluída com base nos requisitos aplicáveis do regulamento identificado na seção B).

A avaliação consiste em (mas não se limita necessariamente a):

- Análise do código fonte,
- Análise documental,
- Verificação da conformidade com os requisitos regulamentares em vigor.

Consulte o Anexo I para obter uma lista detalhada completa dos requisitos testados.

Consulte o Anexo II para obter detalhes relacionados aos testes de RNG.

N) Atividades de teste aplicadas

Procedimento interno seguido:

Rif. "MÉTODOS DE TESTE IOP 02-02".

O) Informações adicionais

Nenhuma

P) Configuração e arquitetura da aplicação/sistema

Consulte a secção K)

Q) Produto testado

Os testes foram realizados nos ficheiros listados abaixo:

Nome do ficheiro	SHA1	Descrição	Crítico	Item de Teste
rng-server	a6f7523a09b72e9b24bfde9772008ff966ad8a75	RNG	Sim	R001
libfortuna-st.a	f729c25b7919ce800344467e9cda816aef53673f	RNG	Sim	R001
fortuna.h	6d3ef3a393e8778b8f27688f691aa7142059f21f	RNG	Sim	R001

R) Revisões do relatório

N.A.

S) CERTIFICAÇÃO

Job ID: BR-PR_ORT001RNG.1_REV.1

Data: 11/11/2024

Requerente: ORTIZ GAMING, S.L.
Calle Pollensa (Ed. Artemisa), 2 – Oficina 25 28290
Las Rozas de Madrid, Madrid, (Spain)

Número total de páginas: **10**

A QUINEL Ltd declara que os itens de teste identificados na secção E) estão em conformidade com o regulamento identificado na secção B).

Consulte o Anexo I para obter a lista completa dos requisitos atendidos.
Consulte o Anexo II para obter detalhes relacionados aos testes de RNG.

T) CONDIÇÕES

Nenhum.

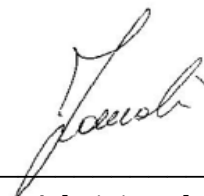
U) CONCLUSÕES

Os jogos /itens de teste identificados na secção E) estão em conformidade com os requisitos aplicáveis das normas técnicas solicitadas.

Data: 11/11/2024

Assinado:

Fabio Valenti – Gerente de Laboratório
(QUINEL Ltd)



Isacco Ceci – Administrador Delegado
(QUINEL Ltd)

ANEXO I - REQUISITOS ATENDIDOS

A menos que especificado de forma diferente, os resultados estão relacionados a todos os itens de teste.

GLI-19 - Standards for Interactive Gaming Systems - v3.0

Capítulo 3: Requisitos do Gerador de Números Aleatórios (RNG)		
3.1 - Introdução	Resultado	Comentários
3.1.1 - Declaração Geral	APLICÁVEL	O item de teste consiste em um RNG baseado em software.
3.2 - Requisitos Gerais de RNG	Resultado	Comentários
3.2.1 - Revisão do Código Fonte	APROVADO	Consulte o Anexo II para obter detalhes relacionados aos testes de RNG.
3.2.2 - Análise estatística	APROVADO	
3.2.3 - Distribuição	APROVADO	
3.2.4 - Independência	APROVADO	
3.2.5 - Resultados Disponíveis	APROVADO	
3.2 - Monitoramento e Força do RNG	Resultado	Comentários
3.3.1 - Força do RNG para Determinar Resultados	APROVADO	
3.3.2 - Ataques Criptográficos ao RNG	APROVADO	Consulte o Anexo II para obter detalhes relacionados aos ataques criptográficos ao RNG.
3.3.3 - Monitoramento de Resultados Dinâmicos para RNGs Baseados em Hardware	NÃO APLICÁVEL	Não aplicável ao item de teste atual (RNG baseado em software).
3.4 - RNG Mecânico (Dispositivo Físico de Aleatoriedade)	Resultado	Comentários
3.4.1 - Declaração Geral	NÃO APLICÁVEL	Não aplicável ao item de teste atual (RNG baseado em software).
3.4.2 - Coleta de Dados	NÃO APLICÁVEL	
3.4.3 - Durabilidade	NÃO APLICÁVEL	
3.4.4 - Manipulação/Adulteração	NÃO APLICÁVEL	

ANEXO II – DETALHES DO TESTE RNG

A) Segurança

O servidor RNG é responsável por lidar com as solicitações e as respostas para dados aleatórios. A segurança da comunicação deve ser avaliada durante os testes do jogo.

B) Ataques criptográficos de RNG

Fortuna é um RNG criptograficamente seguro. Nesta implementação, o gerador é um AES em modo contador. Além disso, um algoritmo SHA-256 hashes a semente.

Ataque Criptoanalítico Direto: Devido à implementação subjacente do AES CSPRNG, esta implementação do algoritmo Fortuna é resistente a este ataque.

Ataque de entrada conhecido: O algoritmo Fortuna fornece um procedimento eficaz para semear e resemear programado para agir em pools de entropia preenchidos de diferentes fontes.

State Compromise Extension Attack: O algoritmo Fortuna fornece um procedimento eficaz para a coleta de entropia, e seu uso na resemeadura o torna resistente a esse ataque.

C) Resultados dos testes para saída bruta de RNG

Confidence level: 95% and 99%

1) Data sets of 3.500.000 outcomes each of raw 32-bit integers

DIEHARD battery of tests

Overall results:

POSITIVE

Test results:

BIRTHDAY SPACINGS 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
SQUEEZE TEST:	PASS
RUNS TEST:	PASS
CRAPS TEST:	PASS

NIST battery of tests:

Overall results:

POSITIVE

Test results:

FREQUENCY:	PASS
BLOCK FREQUENCY:	PASS
CUMULATIVE SUM:	PASS
RUNS:	PASS
LONGEST RUN:	PASS
RANK:	PASS
FFT:	PASS
NONOVERLAPPING TEMPLATE:	PASS
OVERLAPPING TEMPLATE:	PASS
UNIVERSAL:	PASS
APPROXIMATE ENTROPY:	PASS
RANDOM EXCURSIONS:	PASS
RANDOM EXCURSIONS VARIANT:	PASS
SERIAL:	PASS
LINEAR COMPLEXITY:	PASS

D) Resultados dos testes para dados escalonados

Confidence level: 95% and 99%

- 1) Data sets of 300.000 integer outcomes each in the range [0,36] (included)
- 2) Data sets of 300.000 integer outcomes each in the range [0,51] (included)

Overall results: POSITIVE

Test results:

RUNS TESTS:	PASS
FREQUENCY TESTS:	PASS
SERIAL CORRELATION TESTS:	PASS
GAP TESTS:	PASS

E) Resultados dos testes para dados flutuantes

Confidence level: 95% and 99%

- 1) Data sets of 300.000 float outcomes each in the range [0,1)

Overall results: POSITIVE

Test results:

GAP TESTS:	PASS
FREQUENCY TESTS:	PASS
STANDARD DEVIATION TESTS:	PASS
POKER TESTS:	PASS
ORDER TESTS:	PASS

F) Resultados de teste para dados de baralhos embaralhados

QUINEL Ltd

M Space M3 – Zone 3, Central Business District Triq L-Ghajj tan – Nofs – Birkirkara CBD 3060- Malta

info@quinel.com.mt

Confidence level: 95% and 99%

1) Data sets of 150.000 of shuffled decks with cards in the range [0,51] (included)

Overall results:

POSITIVE

Test results:

POKER HAND TESTS:	PASS
CLOSED CYCLE TESTS:	PASS
FREQUENCY TESTS:	PASS
RUNS TESTS:	PASS

Observação: a seção anterior não foi traduzida para evitar distorções de termos técnicos e nomes de testes padrão usados e reconhecidos universalmente.

FIM
DO
RELATÓRIO DE
CONFORMIDADE