

Raport de evaluare pentru: CT Interactive EOOD

Generator de numere aleatorii RNG versiune 6316

Producător:	CT Gaming AD
Denumire RNG:	RNG v6316
Număr raport ATF:	RNG.ROM.CATE.1008.02.01
Număr document:	01
Data:	27 octombrie 2021
Număr de pagini:	11 pagini, inclusiv 2 pagini ale anexei

BMM Spain Testlabs s.l.u.

Conținutul acestui document este strict confidențial. Acesta a fost pregătit de BMM Spain Testlabs, s.l.u. Acesta a fost pregătit de BMM Spania Testlabs s.l.u (BMM) exclusiv pentru examinarea atentă de către CT Interactive EOOD și Oficiul Național pentru Jocuri de Noroc din România (ONJN) și nu poate fi dezvăluit niciunei alte părți fără acordul prealabil în scris al CT Interactive EOOD.

RAPORT DE EVALUARE

Denumire și adresă client:	CT Interactive EOOD 7 Kukush Str., 1345 - Sofia Bulgaria
Număr de referință client:	Prezentarea scrisorii de cerere din data de 19 octombrie 2021
Date de testare:	Data de începere: 19 octombrie 2021 Data de finalizare: 25 octombrie 2021
Descriere produs / joc:	Denumire RNG v. 6316 RNG SEMNĂTURI: Consultați paragraful 5
Categorie testare:	Evaluare RNG
Jurisdicții recomandate:	România
Standarde tehnice utilizate pentru evaluare:	HOTĂRÂREA GUVERNULUI nr. 111/2016 de aprobare a Normelor Metodologice de implementare a Ordonanței de Urgență al Guvernului nr. 77/2009 privind organizarea și funcționarea jocurilor de noroc și de modificare și completare a Deciziei Guvernamentale nr. 298/2013 privind organizarea și funcționarea Oficiului Național pentru Jocuri de Noroc și de amendare a Deciziei Guvernului nr. 870/2009 de aprobare a Normelor Metodologice de aplicare a Ordinului de Urgență al Guvernului nr. 77/2009 și de abrogare a Deciziei Guvernului nr. 870/2009
Locația în care a fost efectuat testul:	BMM Spain Testlabs, s.l.u. Parque Empresarial Vallsolana, Edificio Vinson Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés Barcelona – Spain
Locația în care a fost eliberat raportul:	BMM Spain Testlabs, s.l.u.
Concluzie:	SE APROBĂ
Număr de referință BMM:	CATE.1008
Metodele/Procedurile utilizate:	EURSAM-SPA-MO-41 v2.9
Consultant (Consultanți):	Slava Kolmykov

1. DOMENIUL DE APLICARE AL EVALUĂRII.

CT Interactive EOOD a solicitat BMM să evalueze generatorul de numere aleatorii (RNG) RNG conform cerințelor jurisdicției din România.

- HOTĂRÂREA GUVERNULUI nr. 111/2016 de aprobare a Normelor Metodologice de implementare a Ordonanței de Urgență al Guvernului nr. 77/2009 privind organizarea și funcționarea jocurilor de noroc și de modificare și completare a Deciziei Guvernamentale nr. 298/2013 privind organizarea și funcționarea Oficiului Național pentru Jocuri de Noroc și de amendare a Deciziei Guvernului nr. 870/2009 de aprobare a Normelor Metodologice de aplicare a Ordinului de Urgență al Guvernului nr. 77/2009 și de abrogare a Deciziei Guvernului nr. 870/2009

2. DESCRIEREA RNG.

RNG este o implementare a `dev / urandom` care utilizează algoritmul Fortuna în mediile Linux.

3. EVALUAREA EFECTUATĂ DE BMM.

BMM a examinat codul sursă RNG și a efectuat teste statistice ale rezultatelor produse de RNG. Fișierul (fișierele) relevante utilizate sunt prezentate în secțiunea 5.

3.1. REVIZUIREA CODULUI SURSĂ

Următoarele secțiuni descriu implementarea RNG în codul sursă.

3.1.1 ÎNSĂMÂNȚAREA.

RNG este puternic din punct de vedere criptografic și nu necesită metode ulterioare de însămânțare.

3.1.2 CARACTERUL CICLIC.

RNG este puternic din punct de vedere criptografic și nu este ciclic.

3.1.3 SCALAREA.

Metoda de scalare nu introduce bias.

3.1.4 IMPREVIZIBILITATEA.

RNG este sigur din punct de vedere criptografic.

3.2. TESTARE STATISTICĂ.

Au fost efectuate teste statistice ale rezultatelor produse de RNG. Producția brută de RNG a fost supusă unei serii de teste din grupul Empirice, Diehard și NIST. În anexa A sunt descrise testele efectuate în fiecare grup de teste.

Fiecare test testează ipoteza că RNG este o sursă aleatorie de numere. Este produsă o „valoare P” pentru fiecare rundă de teste, care reprezintă probabilitatea ca un proces cu adevărat aleatoriu să producă același rezultat sau unul mai extrem. Valorile P sunt de așteptat să fie distribuite uniform între 0 și 1. Valorile p pentru fiecare test sunt evaluate folosind un test Anderson-Darling. Acesta produce o singură valoare P, care este probabilitatea ca valorile P individuale să fi fost produse dintr-o distribuție uniformă.

În cele din urmă, valorile P din fiecare test din același grup de teste sunt combinate folosind metoda Holm-Bonferroni pentru a obține o valoare P totală. Acest proces ajustează fiecare valoare P pentru a se asigura că probabilitatea generală de acceptare a RNG ca fiind aleatoriu se potrivește cu intervalul de încredere utilizat. Valoarea P totală, egală cu minimul valorilor P ajustate, este comparată cu o valoare alfa specifică pentru a determina dacă RNG este acceptat sau respins ca fiind aleatoriu pentru un interval de încredere specific.

3.2.1 TESTE EMPIRICE

Eșantionul 1:

Test	Valori P	Încredere 95%	Încredere 99%
Frequency Test (Testul de frecvență)	1.000000	SE APROBĂ	SE APROBĂ
Serial Correlation Test (Testul de corelație serială)	1.000000	SE APROBĂ	SE APROBĂ
Runs Test (Testul secvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Gap Test (Testul decalajelor)	0,583222	SE APROBĂ	SE APROBĂ
Coupon Collector Test (Testul colectorului de cupoane)	1.000000	SE APROBĂ	SE APROBĂ
Subsequences Test (Testul subsecvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Poker Test (Testul Poker)	1.000000	SE APROBĂ	SE APROBĂ
În general	0,583222	SE APROBĂ	SE APROBĂ

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 95% din intervalul de încredere.

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 99% din intervalul de încredere.

Eșantionul 2:

Test	Valori P	Încredere 95%	Încredere 99%
Frequency Test (Testul de frecvență)	1.000000	SE APROBĂ	SE APROBĂ
Serial Correlation Test (Test de corelație serială)	0,856194	SE APROBĂ	SE APROBĂ
Runs Test (Testul secvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Gap Test (Testul decalajelor)	1.000000	SE APROBĂ	SE APROBĂ
Coupon Collector Test (Testul colectorului de cupoane)	0,535097	SE APROBĂ	SE APROBĂ
Subsequences Test (Testul subsecvențelor)	0,585638	SE APROBĂ	SE APROBĂ
Poker Test (Testul Poker)	1.000000	SE APROBĂ	SE APROBĂ
În general	0,535097	SE APROBĂ	SE APROBĂ

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 95% din intervalul de încredere.

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 99% din intervalul de încredere.

3.2.2 BATERIA DE TESTE DIEHARD

Eșantionul 1:

Test	Valori P	Încredere 95%	Încredere 99%
Binary Rank 32x32 Test (Testul de rang binar pentru matrice 32x32)	1.000000	SE APROBĂ	SE APROBĂ
Binary Rank 6x8 Test (Testul de rang binar pentru matrice 6x8)	0,591772	SE APROBĂ	SE APROBĂ
Birthday Spacings Test (Testul distanțelor dintre zilele de naștere)	1.000000	SE APROBĂ	SE APROBĂ
Bitstream Test (Testul fluxului de biți)	0,935545	SE APROBĂ	SE APROBĂ
Count The 1's Stream Test (Testul de numărare a primului flux)	1.000000	SE APROBĂ	SE APROBĂ
Count The 1's Specific Test (Testul de numărare a primului specific)	0,585032	SE APROBĂ	SE APROBĂ
Runs Test (Testul secvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Squeeze Test (Testul Squeeze)	1.000000	SE APROBĂ	SE APROBĂ
În general	0,585032	SE APROBĂ	SE APROBĂ

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 95% din intervalul de încredere.

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 99% din intervalul de încredere.

Eșantionul 2:

Test	Valori P	Încredere 95%	Încredere 99%
Binary Rank 32x32 Test (Test de rang binar pentru matrice 32x32)	0,367154	SE APROBĂ	SE APROBĂ
Binary Rank 6x8 Test (Test de rang binar pentru matrice 6x8)	0,012529	NU SE APROBĂ	SE APROBĂ
Birthday Spacings Test (Testul distanțelor dintre zilele de naștere)	1.000000	SE APROBĂ	SE APROBĂ
Bitstream Test (Testul fluxului de biți)	0,950484	SE APROBĂ	SE APROBĂ
Count The 1's Stream Test (Testul de numărare a primului flux)	1.000000	SE APROBĂ	SE APROBĂ
Count The 1's Specific Test (Test numărarea primului specific)	1.000000	SE APROBĂ	SE APROBĂ
Runs Test (Testul secvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Squeeze Test	0,731405	SE APROBĂ	SE APROBĂ
În general	0,012529	NU SE APROBĂ	SE APROBĂ

Concluzie: RNG este **NU ESTE ACCEPTAT** ca aleatoriu la 95% din intervalul de încredere.

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 99% din intervalul de încredere.

3.2.3 TESTE NIST

Eșantionul 1:

Test	Valori P	Încredere 95%	Încredere 99%
Approximate Entropy Test (Test de estimare aproximativă a entropiei)	1.000000	SE APROBĂ	SE APROBĂ
Block Frequency Test (Testul de frecvență a blocului)	1.000000	SE APROBĂ	SE APROBĂ
Cumulative Sums Test (Testul sumelor cumulate)	1.000000	SE APROBĂ	SE APROBĂ
Discrete Fourier Transform Test (Testul Transformării lui Fourier discretă)	1.000000	SE APROBĂ	SE APROBĂ
Frequency Test (Testul de frecvență)	1.000000	SE APROBĂ	SE APROBĂ
Linear Complexity Test (Testul de complexitate a linearității)	1.000000	SE APROBĂ	SE APROBĂ
Longest Run of Ones Test (Testul celei mai lungi secvențe a numărului unu)	1.000000	SE APROBĂ	SE APROBĂ
Non-Overlapping Template Matchings Test (Testul de potrivire a modelelor nesuprapuse)	1.000000	SE APROBĂ	SE APROBĂ
Overlapping Template Matchings Test (Testul de potrivire a modelelor suprapuse)	1.000000	SE APROBĂ	SE APROBĂ
Random Excursions Test (Testul excursiilor aleatorii)	1.000000	SE APROBĂ	SE APROBĂ
Random Excursions Variant Test (Testul variantelor excursiilor aleatorii)	1.000000	SE APROBĂ	SE APROBĂ
Rank Test (Testul rangurilor)	1.000000	SE APROBĂ	SE APROBĂ
Runs Test (Testul secvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Serial Test (Testul seriialelor)	1.000000	SE APROBĂ	SE APROBĂ
Universal Test (Test universal)	1.000000	SE APROBĂ	SE APROBĂ
În general	1.000000	SE APROBĂ	SE APROBĂ

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 95% din intervalul de încredere.

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 99% din intervalul de încredere.

Eșantionul 2:

Test	Valori P	Încredere 95%	Încredere 99%
Approximate Entropy Test (Test de estimare aproximativă a entropiei)	1.000000	SE APROBĂ	SE APROBĂ
Block Frequency Test (Testul de frecvență a blocului)	1.000000	SE APROBĂ	SE APROBĂ
Cumulative Sums Test (Testul sumelor cumulate)	1.000000	SE APROBĂ	SE APROBĂ
Discrete Fourier Transform Test (Testul Transformării lui Fourier discretă)	1.000000	SE APROBĂ	SE APROBĂ
Frequency Test (Testul de frecvență)	1.000000	SE APROBĂ	SE APROBĂ
Linear Complexity Test (Testul de complexitate a linearității)	1.000000	SE APROBĂ	SE APROBĂ
Longest Run of Ones Test (Testul celei mai lungi secvențe a numărului unu)	1.000000	SE APROBĂ	SE APROBĂ
Non-Overlapping Template Matchings Test (Testul de potrivire a modelelor nesuprapuse)	1.000000	SE APROBĂ	SE APROBĂ
Overlapping Template Matchings Test (Testul de potrivire a modelelor suprapuse)	1.000000	SE APROBĂ	SE APROBĂ
Random Excursions Test (Testul excursiilor aleatorii)	1.000000	SE APROBĂ	SE APROBĂ
Random Excursions Variant Test (Testul variantelor excursiilor aleatorii)	1.000000	SE APROBĂ	SE APROBĂ
Rank Test (Testul rangurilor)	1.000000	SE APROBĂ	SE APROBĂ
Runs Test (Testul secvențelor)	1.000000	SE APROBĂ	SE APROBĂ
Serial Test (Testul seriialelor)	1.000000	SE APROBĂ	SE APROBĂ
Universal Test (Test universal)	1.000000	SE APROBĂ	SE APROBĂ
În general	1.000000	SE APROBĂ	SE APROBĂ

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 95% din intervalul de încredere.

Concluzie: RNG este **ACCEPTAT** ca aleatoriu la 99% din intervalul de încredere.

4. EVALUAREA CERINȚELOR TEHNICE.

BMM a testat și a confirmat conformitatea RNG cu cerințele tehnice aplicabile pentru piața jocurilor de noroc online din România. BMM a efectuat următoarele teste pentru a confirma respectarea specificațiilor de reglementare relevante:

Cerință de reglementare	Detalii	Rezultat Se aprobă / Nu se aprobă /NA	Note
Anexa 7, Capitolul 2, 1.6.	Cererea de autorizare a activității trebuie redactată și scrisă în limba română, trebuie semnată de reprezentantul legal / reprezentantul autorizat al operatorului economic și va conține: - Documente care demonstrează performanța certificărilor pentru programul de jocuri, rata procentuală de acordare teoretică (TAP) și generatorul de numere aleatorii (RNG).	SE APROBĂ	

5. FIȘIERE CODURI SURSĂ.

RNG utilizează următoarele fișiere sursă. Semnăturile furnizate sunt generate cu ajutorul SHA1.

Fișier	SHA1
LinuxUrandom.pm	D6893CAA6F2B2A8414C67BA2140F08C19D3C73CE
LinuxUrandomQueue.pm	DEE2C8460E56767EAA7EEB776F176EECBA00CEF7
RNG.pm	B5ADAA3D6C44132799960B36889B2D9224553EF8

6. INFORMAȚII/OBSERVAȚII SUPLIMENTARE.

Acest raport a fost întocmit pentru a schimba dreptul de proprietate al clientului asupra produsului în CT Interactive EOOD.

7. CONCLUZII.

Conform rezultatelor testelor¹ obținute, BMM Spain Testlabs s.l.u. confirmă că elementul supus testării respectă toate prevederile Normelor amintite în secțiunea Domeniul de aplicare al evaluării.

Cu stimă,

Patricia García

Director al Services Delivery EURSAM

¹ Rezultatele incluse în acest document se referă exclusiv la eșantioanele testate, așa cum se descrie în secțiunea corespunzătoare.

Acest raport de testare nu poate fi reprodus sub alte forme, decât integral, cu excepția permisiunii scrise acordate de BMM Spain Testlabs, s.l.u.

ANEXA A: TESTE STATISTICE

Testele următoare au fost utilizate pentru a testa proprietățile statistice ale RNG.

Teste empirice

Testele empirice se bazează pe testele descrise de Donald Knuth în „The Art of Computer Programming Volume 2: Seminumerical Algorithms (1968, revizuită în 1997)”. Acestea testează secvențe de numere scalate la intervale specifice.

Frequency Test (Testul de frecvență)	De câte ori fiecare număr apare în setul eșantion.
Serial Correlation Test (Testul de corelație serială)	De câte ori apar împreună grupuri de numere care nu se suprapun. Grupurile de două, trei sau patru sunt testate separat.
Runs Test (Testul secvențelor)	Numărul de secvențe ascendente și descendente ale numerelor. Rețineți că acesta este un test diferit de testul Runs din testele Diehard și NIST.
Gap Test (Testul decalajelor)	Numărul de dimensiuni ale decalajelor dintre aparițiile succesive ale unui număr dat. Fiecare număr din interval este testat separat.
Coupon Collector Test (Testul colectorului de cupoane)	Numărul de lungimi de secvență necesare pentru a completa un set complet al fiecărui număr din interval.
Subsequences Test (Testul subsecvențelor)	Similar testului Serial Correlation (corelație serială) pentru perechi de numere, cu excepția faptului că se consideră numerele separate printr-un decalaj specific. Dimensiunile pașilor de 5, 10, 15 și 20 sunt testate separat.
Poker Test (Testul Poker)	Secvența este împărțită în grupuri de cinci. Este numărat numărul valorilor unice din fiecare grup.

Bateria de teste Diehard

Testele DieHard se bazează pe suita de teste publicate de George Marsaglia în 1995. Acestea testează secvențe de rezultate binare brute produse de RNG.

Binary Rank 32x32 Test (Testul de rang binar pentru matrice 32x32)	Matricele sunt create utilizând cuvinte de 32 x 32 biți. Sunt numărate rangurile matricelor rezultate.
Binary Rank 6x8 Test (Testul de rang binar pentru matrice 6x8)	Ca și testul Binary Rank 32x32, cu excepția faptului că fiecare matrice este formată utilizând 6 valori, fiecare luând 8 biți din cuvinte de 32 de biți cu un offset specific. Toate offset-urile posibile sunt testate separat.
Birthday Spacings Test (Testul distanțelor dintre zilele de naștere)	Valorile pe 26 de biți sunt preluate din cuvinte succesive pe 32 de biți cu un offset specific. Valorile sunt sortate și sunt calculate distanțele dintre ele. Este numărat numărul de distanțe de aceeași dimensiune. Toate offset-urile posibile sunt testate separat.
Bitstream Test (Testul fluxului de biți)	Blocurile de valori de 2^{18} sunt tratate ca un flux de valori care se suprapun pe 20 de biți. Este numărat numărul de valori posibile de 20 de biți care nu se găsesc în fiecare bloc.
Count The 1's Stream Test (Testul de numărare a primului flux)	Sunt luate valori de 8 biți și li se atribuie o „literă” în funcție de numărul apariției uneia în reprezentarea binară a fiecărei valori. Sunt numărate grupurile suprapuse de „5 litere”.

Count The 1's Specific Test (Testul de numărare a primului specific)	Asemănător cu Testul Count The 1's Stream, cu excepția faptului că valorile de 8 biți sunt preluate din cuvinte succesive de 32 de biți cu un offset specific. Toate offset-urile posibile sunt testate separat.
Runs Test (Testul secvențelor)	Numără secvențe crescătoare și descrescătoare de cuvinte de 32 de biți. Rețineți că acesta este un test diferit de testul Runs din testele Empirice și NIST.
Squeeze Test (Testul Squeeze)	O valoare de 2^{31} este înmulțită în mod repetat cu cuvinte de 32 de biți, împărțind cu 2^{32} și luând valoarea maximă a rezultatului de fiecare dată. Este numărat numărul de cuvinte succesive care sunt necesare pentru a reduce valoarea până la 1. Valoarea este resetată la 2^{31} și procesul este repetat.

Teste NIST

Testele NIST se bazează pe setul de teste lansate de Institutul Național de Standarde și Tehnologie în Publicația Specială 800-22, Revizia 1a (revizuită în aprilie 2010). Acestea testează secvențe de rezultate binare brute produse de RNG.

Approximate Entropy Test (Testul de estimare aproximativă a entropiei)	Similar testului Serial Test, numără fiecare valoare posibilă de biți m , cu excepția faptului că o face pentru două lungimi adiacente de biți m și le compară pe cele două.
Block Frequency Test (Testul de frecvență a blocului)	Similar testului Frequency Test, cu excepția faptului că datele sunt împărțite în blocuri de dimensiuni egale. Este numărat numărul de cifre unu și zero din fiecare bloc.
Cumulative Sums Test (Testul sumelor cumulate)	Sunt create intervale aleatorii transformând datele în $+1 / -1$ pentru $1 / 0$ și adunând valori consecutive.
Discrete Fourier Transform Test (Testul Transformării lui Fourier discretă)	Datele sunt transformate folosind transformarea lui Fourier discretă. Este numărat numărul de vârfuri între limita de 95%.
Frequency Test (Testul de frecvență)	Este numărat numărul de cifre unu și zero din output-ul binar.
Linear Complexity Test (Testul de complexitate a linearității)	Este determinată lungimea complexității liniare a secvenței aleatorii.
Longest Run of Ones Test (Testul celei mai lungi secvențe a numărului unu)	Datele sunt împărțite în blocuri de dimensiuni egale. Este determinată și numărată cea mai lungă secvență a numărului unu din fiecare bloc.
Non-Overlapping Template Matchings Test (Testul de potrivire a modelelor nesuprapuse)	Datele sunt împărțite în blocuri de dimensiuni egale. În fiecare bloc este căutat un model specific de biți și este numărat. Este rulat un test separat pentru diferite modele de biți. Fiecare model de biți căutat nu se suprapune cu el însuși. Adică, atunci când modelul este potrivit, sfârșitul modelului nu poate fi începutul unei alte potriviri.
Overlapping Template Matchings Test (Testul de potrivire a modelelor suprapuse)	Similar cu testul Non-Overlapping Template Matchings, cu excepția că este căutat un singur model, care se poate suprapune cu el însuși.
Random Excursions Test (Testul excursiilor aleatorii)	La fel ca în cazul testului Cumulative Sums, intervalele aleatorii sunt create prin transformarea datelor în $+1 / -1$ pentru $1 / 0$, respectiv și însumarea valorilor consecutive. Este numărat de câte ori este vizitată o anumită stare între revenirile la zero. Se efectuează teste separate pentru diferite stări de la -4 la $+4$, neincluzând 0.
Random Excursions Variant Test (Testul variantelor excursiilor aleatorii)	Similar cu testul Random Excursions, cu excepția faptului că este numărat de câte ori este vizitată o anumită stare pentru întreaga secvență. Se efectuează teste separate pentru diferite stări de la -9 la $+9$, neincluzând 0.
Rank Test (Testul rangurilor)	Matricele sunt create utilizând cuvinte de 32×32 biți. Sunt numărate rangurile matricelor rezultate. Rețineți că acesta este în mod fundamental același test ca testul Binary Rank 32×32 din testele Diehard, deși implementarea poate diferi.

Runs Test (Testul secvențelor)	Sunt numărate secvențe de biți consecutivi cu aceeași valoare de diferite lungimi.
Serial Test (Testul seriialelor)	Numără fiecare valoare posibilă a bitului m. Se efectuează teste separate pentru diferite lungimi de biți m.
Universal Test (Test universal)	Sunt numărate distanțele dintre modelele repetate ale biților.