

Raport de evaluare pentru Amarix B.V.

AMARIX-RNG Versiune 1.0.0

Producător:	Amarix B.V.
Număr raport ATF:	RNG.ROM.RES-OL.1001.01.01
Număr document:	01
Data:	24 mai 2024
Număr de pagini:	9

BMM Spain Testlabs s.l.u.

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



INFORMAȚII GENERALE

Numele și adresa solicitantului:	Amarix B.V. Schottegatweg Oost 10 Unit 1-9, Bon Bini Business Center, Curaçao
Număr de referință solicitant:	Prezentarea scrisorii de cerere din data de 23 februarie 2024
Date de testare:	Data de începere: 25 martie 2024 Data de finalizare: 19 aprilie 2024
Tip de evaluare	Evaluare statistică
Stilul produsului:	Software RNG
Descrierea produsului:	AMARIX-RNG
Nume:	Versiune 1.0.0
Versiune:	SEMNĂTURI: A se vedea secțiunea 2.2
Categorie testare:	Categoria 0
Jurisdicții recomandate:	România
Standard tehnic / Regulament utilizat pentru evaluare:	HOTĂRÂRE DE GUVERN nr. 111/2016 pentru aprobarea Normelor metodologice de aplicare a Ordonanței de urgență a Guvernului nr. 77/2009 privind organizarea și exploatarea jocurilor de noroc și pentru modificarea și completarea Hotărârii Guvernului nr. 298/2013 privind organizarea și funcționarea Oficiului Național pentru Jocuri de Noroc și pentru modificarea Hotărârii Guvernului nr. 870/2009 privind aprobarea Normelor metodologice de aplicare a Ordonanței de urgență a Guvernului nr. 77/2009 și pentru abrogarea Hotărârii Guvernului nr. 870/2009.
Locația în care a fost efectuat testul:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana, 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. Edificio Vinson del Parque Empresarial Vallsolana, Camí de Can Camps 17-19, 08174 Sant Cugat del Vallés - Barcelona, Spain
Concluzia evaluării	SE APROBĂ
Număr de ref. BMM:	RES-OL.1001
Metode/Procedee utilizate:	EURSAM-SPA-MO-41 3.0
Ingineri de testare:	Miguel Oliveira

1. DOMENIUL DE APLICARE AL EVALUĂRII.

Amarix B.V. a solicitat evaluarea produselor indicate în secțiunea 2 pentru operarea pe piața relevantă din România:

- România – HOTĂRÂRE DE GUVERN nr. 111/2016 pentru aprobarea Normelor metodologice de aplicare a Ordonanței de urgență a Guvernului nr. 77/2009 privind organizarea și exploatarea jocurilor de noroc și pentru modificarea și completarea Hotărârii Guvernului nr. 298/2013 privind organizarea și funcționarea Oficiului Național pentru Jocuri de Noroc și pentru modificarea Hotărârii Guvernului nr. 870/2009 privind aprobarea Normelor metodologice de aplicare a Ordonanței de urgență a Guvernului nr. 77/2009 și pentru abrogarea Hotărârii Guvernului nr. 870/2009.

2. CARACTERISTICILE EVALUĂRII.

2.1. DESCRIEREA PRODUSULUI.

Software-ul RNG din sistem este serviciul RNG. Acesta este găzduit într-un cluster Kubernetes pe un server virtual din centrul de date. Serviciul RNG este scris în Java 17 și utilizează biblioteca org.apache.commons:commons-rng-simple:1.5 din depozitul Maven Central.

Atunci când serviciul este lansat, 64 de octeți aleatorii sunt citați din sursa /dev/urandom, care sunt utilizați ca seminte pentru algoritmul ISAAC. La fiecare solicitare a unui număr aleatoriu, serviciul RNG returnează 32 de octeți aleatorii generați de algoritmul ISAAC. Acest număr este utilizat ca sămânță pentru următoarele etape.

Fiecare joc are, de asemenea, un șir de caractere specificat în configurație. Octeții obținuți sunt supuși funcției hash: hash sha256 în bucle de 1000 de iterații. Hash este combinat cu clientSeed și nonce primit de la jucător pentru a obține un număr aleatoriu. Șirul de caractere rezultat este un șir hexa de 64 de caractere (256 de biți) care va fi utilizat direct de logica jocului pentru a produce rezultatele jocului.

2.2. SOFTWARE EVALUAT.

Produs: AMARIX-RNG v1.0.0					
Denumirea fișierului	Versiune	Locație	Funcție	Tip semnătură digitală	Semnătură digitală
rng-sbai-certified.jar	1.0.0	Server	RNG	SHA-1	98846A088426F85600EE32DEF1AB6A6AE90B3916
rng-sbai-certified-sources.jar	1.0.0	Sursa	Sursa RNG	SHA-1	8354EC44F14D0AC0FA1205F75B7A665A1D9F08A7

2.3. REVIZUIREA CODULUI SURSĂ.

BMM a examinat codul sursă RNG și a efectuat teste statistice ale rezultatelor produse de RNG. Fișierul (fișierele) relevante utilizate sunt prezentate în secțiunea 2.2.

2.3.1. ÎNSĂMÂNȚAREA.

Algoritmul ISAAC (însămânțat de la sursa /dev/urandom) produce o sămânță aleatorie.

2.3.2. CARACTERUL CICLIC.

Algoritmul este însămânțat la fiecare 1000 de numere solicitate.

2.3.3. SCALAREA.

Algoritmul nu produce niciun algoritm de scalare.

2.3.4. IMPREVIZIBILITATEA.

RNG folosește sha256 pentru a produce rezultate imprevizibile.

2.4. 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.

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.

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)	0,909765	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	0,909765	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.

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)	Cuvintele de 32 de biți sunt luate ca valori, sunt sortate și sunt calculate distanțele dintre acestea. Este numărat numărul de distanțe de aceeași dimensiune.
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.

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)	1,000000	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)	1,000000	SE APROBĂ	SE APROBĂ
Count The 1's Stream Test (Testul de numărare a primului flux)	0,071261	SE APROBĂ	SE APROBĂ
Count The 1's Specific Test (Testul de numărare a primului specific)	1,000000	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	0,071261	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.

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 x 32 biți. Sunt numărate rangurile matricelor rezultate. Rețineți că acesta este în mod fundamental același test ca testul Binary Rank 32x32 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.

Test	Valori P	Încredere 95%	Încredere 99%
Approximate Entropy Test (Testul 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)	0,146020	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	0,146020	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. EVALUAREA EFECTUATĂ DE BMM.

BMM a testat și a confirmat conformitatea AMARIX-RNG versiunea 1.0.0 cu cerințele tehnice aplicabile corespunzătoare aplicabile pe piața jocurilor de noroc la distanță din România. BMM a efectuat următoarele teste pentru a confirma respectarea specificațiilor de reglementare în vigoare:

HOTĂRÂREA GUVERNULUI nr. 111/2016 pentru aprobarea Normelor Metodologice de punere în aplicare a Ordonanței de urgență a Guvernului nr. 77/2009 privind organizarea și exploatarea jocurilor de noroc și pentru modificarea și completarea Hotărârii Guvernului nr. 298/2013 privind organizarea și funcționarea Oficiului Național pentru Jocuri de Noroc și pentru modificarea Hotărârii Guvernului nr. 870/2009 pentru aprobarea Normelor metodologice de aplicare a Ordonanței de urgență a Guvernului nr. 77/2009 și pentru abrogarea Hotărârii Guvernului nr. 870/2009 privind organizarea și exploatarea jocurilor de noroc.	Rezultate		
	Ok	Nu se aprobă	Observații
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)	X	☐	RNG a fost evaluat în raport cu standardul GLI-19 v3.0.

4. INFORMAȚII/OBSERVAȚII SUPLIMENTARE.

N/A

5. CONCLUZII.

Conform rezultatelor testelor¹obținute, BMM Spain Testlabs s.l.u. confirmă că elementul supus testării respectă toate prevederile Normelor amintite în secțiunea „1” a acestui raport.

Cu stimă,

Rubén Baptista

SVP Operations EURSAM

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

Acest raport de test nu poate fi reprodus decât în întregime, cu excepția permisiunii scrise prealabile a emitentului - BMM Spain Testlabs, s.l.u.

bmmtestlabs