Bewertungsbericht für
NSUS Malta Limited
Zufallszahlengenerator
Poker Game RNG v 2.0.0

Hersteller:	**NSUS Lab Korea LLC**
ATF-Berichtsnummer:	**RNG.NET.GGNE.1043.02.01**
Dokumentennr.:	**01**
Datum:	**27. Juli 2023**
Anzahl der Seiten:	**9**

BMM Spain Testlabs s.l.u.

ALLGEMEINE INFORMATIONEN

Kundenname und -anschrift:	NSUS Malta Limited Level 3 (suite no: 2386), Tower Business Centre, Tower Street, Swatar, Birkirkara BKR4013, Malta.
Kundenreferenznummer:	AntragsAnforderungsschreiben vom 12. Juli 2023
Testtermine:	Startdatum: 12. Juli 2023 Enddatum: 21. Juli 2023
Beschreibung des Produkts/Spiels:	Poker Game RNG v 2.0.0 RNG SIGNATUREN: Siehe Abschnitt 2.3
Testkategorie:	Kategorie 0
Empfohlene Gerichtsbarkeiten:	Niederlande
Verwendeter technischer Standard für die Bewertung:	▪ Konformitätsbewertungsschema für Online-Glücksspiele der niederländischen Glückspielbehörde - Version 2.0
Ort der Testausführung:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés - Barcelona (Spanien)
Ort der Berichtserstellung:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés - Barcelona (Spanien)
Fazit:	Bestanden
BMM-Referenznummer:	GGNE.1043
Verwendete Methode/Verfahren:	EURSAM-SPA-MO-74 v1.2
Berater:	Luca Borchini

1. UMFANG DER BEWERTUNG.

NSUS Malta Limited hat BMM Spain Testlabs s.l.u., im Folgenden BMM genannt, hat darum gebeten, die in Abschnitt 2 aufgeführten Produkte für den Betrieb auf dem niederländischen Remote Gambling Markt gemäß den nachfolgend beschriebenen Normen/Vorschriften zu bewerten:

- Konformitätsbewertungsschema für Online-Glücksspiele der niederländischen Glückspielbehörde - Version 2.0

2. BEWERTUNGSMERKMALE.

BMM untersuchte den RNG-Quellcode und führte statistische Tests mit der Ausgabe des RNG durch.

2.1. ÜBERPRÜFUNG DES QUELLCODES.

Der RNG basiert auf dem Windows CryptoGenRandom, der ein allgemein anerkannter RNG ist.

2.1.1. SEEDING

Intern platziert. Der RNG ist kryptografisch stark und die Reseeding-Methode ist nicht erforderlich, um Vorhersehbarkeit zu vermeiden.

2.1.2. ZYKLIEREN

Der RNG zykliert nicht, und die Sequenzen sind nicht reproduzierbar.

2.1.3. SKALIEREN

Die Skalierungsmethode führt nicht zu Verzerrungen.

2.1.4. UNVORHERSAGBARKEIT

Der RNG ist kryptographisch sicher.

2.1.5. MAXIMALE LAST

BMM führte mehrere Tests durch, um zu prüfen, ob der RNG während des maximalen Lastzustands weiterhin wie erwartet funktioniert. Die Tests bestehen aus:

- Baseline-Test: Ausführen von Kurzzeittests, um Basismesswerte für den RNG-Dienst zu erhalten.
- Stresstest: Ausführung mit Lasterhöhung, bis die Grenzen des Dienstes erreicht sind.
- Lasttest: Ausführung mit einer mäßig schweren Last über die Zeit.
- Spike-Test: Ausführung mit hohen Belastungsspitzen, um die Stabilität und die Erholungsfähigkeit zwischen den Schüben hoher Aktivität zu überwachen.
- Eintauchtest: Durchführung eines Langzeittests, um mögliche Speicherlecks und andere latente Probleme zu erkennen.

Der RNG hat alle statistischen Tests der Probe bestanden, die in der maximalen Belastung erhalten wurden.

2.1.6. ÜBERWACHUNGSSYSTEM.

Die Ausgabe des RNG wird kontinuierlich überwacht und gegen den gültigen Bereich für jedes Spiel geprüft. Wenn ein RNG-Fehler erkannt wird, löst das interne Überwachungssystem einen Alarm aus und der Spieltisch, der von dem RNG-Fehler betroffen ist, wird gesperrt.

2.2. STATISTISCHES TESTEN.

Jeder Test testet die Hypothese, dass der RNG eine Zufallsquelle für Zahlen ist. Für jeden Testlauf wird ein „P-Wert“ erzeugt, der die Wahrscheinlichkeit angibt, dass ein echter Zufallsprozess das gleiche oder ein extremeres Ergebnis erzeugen würde. Es wird erwartet, dass die P-Werte gleichmäßig zwischen 0 und 1 verteilt sind. Die P-Werte für jeden Test werden mit einem Anderson-Darling-Test ausgewertet. Dies ergibt einen einzigen P-Wert, der die Wahrscheinlichkeit darstellt, dass die einzelnen Pp-Werte aus einer Gleichverteilung erzeugt wurden.

Schließlich werden die Pp-Werte von jedem Test in derselben Prüfsuite unter Verwendung der Holm-Bonferroni-Methode kombiniert, um einen Gesamt-P-Wert zu erhalten. Dieser Prozess passt jeden P-Wert an, um sicherzustellen, dass die Gesamtwahrscheinlichkeit, den RNG als zufällig anzunehmen, mit dem verwendeten Konfidenzintervall übereinstimmt. Der gesamte P-Wert, der dem Minimum der angepassten P-Werte entspricht, wird mit einem bestimmten Alpha-Wert verglichen, um zu bestimmen, ob der RNG als zufällig für ein bestimmtes Konfidenzintervall akzeptiert oder abgelehnt wird.

Empirische Tests

Test	P-Werte	95 % Konfidenz	99 % Konfidenz
Frequenztest	0,755247	BESTANDEN	BESTANDEN
Serieller Korrelationstest	1,000000	BESTANDEN	BESTANDEN
Run-Test	1,000000	BESTANDEN	BESTANDEN
Lückentest	1,000000	BESTANDEN	BESTANDEN
Couponsammler-Test	1,000000	BESTANDEN	BESTANDEN
Subsequenztest	0,568695	BESTANDEN	BESTANDEN
Poker-Test	1,000000	BESTANDEN	BESTANDEN
Gesamt	**0,568695**	**BESTANDEN**	**BESTANDEN**

Fazit: Der RNG wird mit dem 95 %-Konfidenzintervall als zufällig **AKZEPTIERT**.
Fazit: Der RNG wird mit dem 99 %-Konfidenzintervall als zufällig **AKZEPTIERT**

Die empirischen Tests basieren auf den Tests, die von Donald Knuth in The Art of Computer Programming Volume 2 beschrieben wurden: Seminumerische Algorithmen (1968, überarbeitet 1997). Sie prüfen Folgen von Zahlen, die auf bestimmte Bereiche skaliert sind.

Frequenztest	Zählungen der einzelnen Zahlen, die im gesamten Stichprobensatz vorkommen.
Serieller Korrelationstest	Zählungen von nicht überlappenden Gruppen von Zahlen, die zusammen auftreten. Gruppengrößen von zwei, drei und vier werden separat getestet.
Run-Test	Zählen von aufsteigenden und absteigenden Zahlenfolgen. Beachten Sie, dass dies ein anderer Test ist als der Run-Test in den Diehard- und NIST-Tests.
Lückentest	Zählt die Größe der Lücken zwischen aufeinanderfolgenden Vorkommen einer bestimmten Zahl. Jede Zahl im Bereich wird separat getestet.
Couponsammler-Test	Zählung der Sequenzlängen, die erforderlich sind, um einen vollständigen Satz jeder Zahl im Bereich zu vervollständigen.
Subsequenztest	Ähnlich wie der Serienkorrelationstest für Zahlenpaare, nur dass hier Zahlen betrachtet werden, die durch eine bestimmte Lücke getrennt sind. Schrittweiten von 5, 10, 15 und 20 werden separat getestet.
Poker-Test	Die Sequenz wird in Fünfergruppen aufgeteilt. Es wird die Anzahl der eindeutigen Werte in jeder Gruppe gezählt.

Diehard-Tests

Test	P-Werte	95 % Konfidenz	99 % Konfidenz
Binär-Rang 32x32-Test	1,000000	BESTANDEN	BESTANDEN
Binär-Rang 6x8-Test	0,762934	BESTANDEN	BESTANDEN
Geburtstagsabstände-Test	1,000000	BESTANDEN	BESTANDEN
Bitstream-Test	1,000000	BESTANDEN	BESTANDEN
Zähle die Einsen Stream-Test	1,000000	BESTANDEN	BESTANDEN
Zähle die Einsen spezifischer Test	1,000000	BESTANDEN	BESTANDEN
Run-Test	1,000000	BESTANDEN	BESTANDEN
Squeeze-Test	1,000000	BESTANDEN	BESTANDEN
Gesamt	**0,762934**	**BESTANDEN**	**BESTANDEN**

Fazit: Der RNG wird mit dem 95 %-Konfidenzintervall als zufällig **AKZEPTIERT**.
Fazit: Der RNG wird mit dem 99 %-Konfidenzintervall als zufällig **AKZEPTIERT**.

Die Diehard-Tests basieren auf der 1995 von George Marsaglia veröffentlichten Testsuite. Sie testen Sequenzen der rohen Binärausgabe des RNGs.

Binär-Rang 32x32-Test	Matrizen werden mit 32 32-Bit-Worten erstellt. Die Ränge der resultierenden Matrizen werden gezählt.
Binär-Rang 6x8-Test	Wie der Binary Rank 32x32 Test, nur dass jede Matrix aus 6 Werten gebildet wird, die jeweils 8 Bits aus aufeinanderfolgenden 32-Bit-Wörtern mit einem bestimmten Offset nehmen. Alle möglichen Offsets werden separat getestet.
Geburtstagsabstände-Test	26-Bit-Werte werden aus aufeinanderfolgenden 32-Bit-Worten mit einem bestimmten Offset entnommen. Die Werte werden sortiert und die Abstände zwischen ihnen berechnet. Es wird die Anzahl der gleich großen Abstände gezählt. Alle möglichen Offsets werden separat getestet.
Bitstream-Test	Blöcke von 2^18 Werten werden als ein Strom von überlappenden 20-Bit-Werten behandelt. Es wird die Anzahl der möglichen 20-Bit-Werte gezählt, die in jedem Block nicht gefunden werden.
Zähle die Einsen Stream-Test	8-Bit-Werte werden genommen und einem „Buchstaben“ zugeordnet, basierend auf der Anzahl der Einsen, die in der binären Darstellung jedes Wertes erscheinen. Überlappende Gruppen von 5 „Buchstaben“ werden gezählt.
Zähle die Einsen spezifischer Test	Ähnlich wie der Zähle die Einsen Stream-Test, nur dass 8-Bit-Werte aus aufeinanderfolgenden 32-Bit-Wörtern mit einem bestimmten Offset genommen werden. Alle möglichen Offsets werden separat getestet.
Run-Test	Zählt Folgen von auf- und absteigenden 32-Bit-Wörtern. Beachten Sie, dass dies ein anderer Test ist als der Run-Test in den empirischen und NIST-Tests.
Squeeze-Test	Ein Wert von 2^31 wird wiederholt mit 32-Bit-Wörtern multipliziert, dabei wird durch 2^32 geteilt und jedes Mal die Obergrenze des Ergebnisses genommen. Es wird die Anzahl der aufeinanderfolgenden Worte gezählt, die erforderlich sind, um den Wert auf 1 zu reduzieren. Der Wert wird auf 2^31 zurückgesetzt und der Vorgang wird wiederholt.

NIST-Tests

Test	P-Werte	95 % Konfidenz	99 % Konfidenz
Approximativer Entropie-Test	1,000000	BESTANDEN	BESTANDEN
Blockfrequenztest	1,000000	BESTANDEN	BESTANDEN
Kumulativsummen-Test	1,000000	BESTANDEN	BESTANDEN
Diskreter Fourier-Transformationstest	1,000000	BESTANDEN	BESTANDEN
Frequenztest	1,000000	BESTANDEN	BESTANDEN
Linearer Komplexitätstest	1,000000	BESTANDEN	BESTANDEN
Längster Lauf des Einser-Tests	1,000000	BESTANDEN	BESTANDEN
Test auf nicht-überlappende Vorlagenübereinstimmungen	1,000000	BESTANDEN	BESTANDEN
Test auf überlappende Vorlagenübereinstimmungen	1,000000	BESTANDEN	BESTANDEN
Test für zufällige Exkursionen	1,000000	BESTANDEN	BESTANDEN
Zufällige Exkursionen Variantentest	1,000000	BESTANDEN	BESTANDEN
Rangfolge-Test	1,000000	BESTANDEN	BESTANDEN
Run-Test	0,530335	BESTANDEN	BESTANDEN
Serieller Test	1,000000	BESTANDEN	BESTANDEN
Universaltest	1,000000	BESTANDEN	BESTANDEN
Gesamt	**0,530335**	**BESTANDEN**	**BESTANDEN**

Fazit: Der RNG wird mit dem 95 %-Konfidenzintervall als zufällig **AKZEPTIERT**.
Fazit: Der RNG wird mit dem 99 %-Konfidenzintervall als zufällig **AKZEPTIERT**.

Die NIST-Tests basieren auf der Testreihe, die vom National Institute of Standards and Technology in der Special Publication 800-22, Revision 1a (überarbeitet April 2010) veröffentlicht wurde. Sie testen Sequenzen der rohen Binärausgabe des RNGs.

Approximativer Entropie-Test	Ähnlich wie beim Serientest wird jeder mögliche m-Bit-Wert gezählt, nur dass dies für zwei benachbarte m-Bit-Längen geschieht und die beiden verglichen werden.
Blockfrequenztest	Ähnlich wie der Frequenztest, nur dass die Daten in gleich große Blöcke aufgeteilt werden. Die Anzahl der Einsen und Nullen in jedem Block wird gezählt.
Kumulativsummen-Test	Zufallsverläufe werden erzeugt, indem die Daten in +1 / -1 für 1 / 0 umgewandelt werden und aufeinanderfolgende Werte summiert werden.
Diskreter Fourier-Transformationstest	Die Daten werden mit einer Diskreten Fourier-Transformation transformiert. Es wird die Anzahl der Peaks innerhalb der 95%-Schwelle gezählt.
Frequenztest	Es wird die Anzahl der Einsen und Nullen in der Binärausgabe gezählt.
Linearer Komplexitätstest	Die Länge der linearen Komplexität der Zufallsfolge wird bestimmt.
Längster Lauf des Einser-Tests	Die Daten werden in gleichgroße Blöcke aufgeteilt. Der längste Lauf von Einsen in jedem Block wird ermittelt und gezählt.
Test auf nicht-überlappende Vorlagenübereinstimmungen	Die Daten werden in gleichgroße Blöcke aufgeteilt. Jeder Block wird nach einem bestimmten Muster von Bits durchsucht und gezählt. Für verschiedene Bitmuster wird ein separater Test durchgeführt. Jedes gesuchte Bitmuster überschneidet sich nicht mit sich selbst. Das heißt, wenn das Muster übereinstimmt, kann das Ende des Musters nicht der Anfang einer anderen Übereinstimmung sein.
Test auf überlappende Vorlagenübereinstimmungen	Ähnlich wie der Test für nicht überlappende Vorlagenübereinstimmungen, nur dass nur ein Muster gesucht wird, das sich mit sich selbst überlappen kann.

Test für zufällige Exkursionen	Wie beim Kumulativsummentest werden Zufallsverläufe erzeugt, indem die Daten in +1 / -1 für 1 / 0 umgewandelt werden und aufeinanderfolgende Werte summiert werden. Es wird gezählt, wie oft ein bestimmter Zustand zwischen den Rücksprüngen auf Null auftritt. Es werden getrennte Tests für verschiedene Zustände von -4 bis +4 durchgeführt, wobei 0 nicht eingeschlossen ist.
Zufällige Exkursionen Variantentest	Ähnlich wie der Zufällige Exkursionen-Test, außer dass die Anzahl des Auftretens des gegebenen Zustands für die gesamte Sequenz gezählt wird. Es werden getrennte Tests für verschiedene Zustände von -9 bis +9 durchgeführt, wobei 0 nicht eingeschlossen ist.
Rangfolge-Test	Matrizen werden mit 32 32-Bit-Worten erstellt. Die Ränge der resultierenden Matrizen werden gezählt. Beachten Sie, dass dies grundsätzlich derselbe Test ist wie der Binary Rank 32x32 Test in den Diehard-Tests, auch wenn die Implementierung unterschiedlich sein kann.
Run-Test	Es werden Läufe von aufeinanderfolgenden Bits mit gleichem Wert unterschiedlicher Länge gezählt.
Serieller Test	Zählt alle möglichen m-Bit-Werte. Es werden getrennte Tests für verschiedene m-Bit-Längen durchgeführt.

2.3. EVALUIERTE SOFTWARE.

Produkt: Poker Game RNG v 2.0.0					
Dateiname	**Version**	**Ort**	**Funktion**	**Digitaler Signaturtyp**	**Digitale Signatur**
Rhyme.Random.dll	v2.0.0	Server	RNG	SHAI1	4767A09FD6B1857B288BA642A4B39954AD52092D

2.4. BEWERTUNGSPROZESS

Durchgeführte Bewertung	**Beschreibung des Bewertungsprozesses**
Quellcodeanalyse	Eine Überprüfung des Quellcodes wurde durchgeführt, um sicherzustellen, dass die Quellcode-Implementierung mit den Spielregeln übereinstimmt, die Spiele den verifizierten RNG verwenden und dass keine verdächtigen und nicht konformen Funktionen im Code enthalten sind.
RNG-Softwarebewertung	Empirische Tests an Proben von 1.000.000 Werten des Bereichs 16, 32, 52, 100, 111, 503, 1000. Diehard- und NIST-Testsuiten wurden mit 10.000.000 Rohwerten durchgeführt. Die Ergebnisse dieser Tests wurden mit der Holm-Bonferroni-Methode kombiniert.
Compliance-Bewertung	Ein Funktionstest des Systems, um die korrekte Funktion gemäß den jeweiligen Anforderungen sicherzustellen.
Generierung digitaler Signaturen	Baselining der kritischen Binärdateien durch Generierung der SHA1-Signatur jeder kritischen Datei.
Prüfung der Richtlinien und Dokumente des Betreibers	Überprüfung der Richtlinien und Dokumente des Betreibers, um zu überprüfen, ob die angegebenen Richtlinien und Informationen des Betreibers die einschlägigen Anforderungen erfüllen.

2.5. VOM KUNDEN ÜBERMITTELTE DOKUMENTE

Name des Dokuments und Versionsnummer	Übermitteltes Dokument
Rhyme.Random.dll	Quellcode

3. BMM-BEWERTUNG DURCHGEFÜHRT.

BMM hat die Konformität der in Abschnitt 2 genannten Produkte mit den entsprechenden anwendbaren technischen Anforderungen für den niederländischen Remote-Glücksspielmarkt geprüft und bestätigt. BMM führte folgende Tests durch, um die Einhaltung der einschlägigen regulatorischen Vorgaben zu bestätigen:

NIEDERLÄNDISCHE VORSCHRIFTEN UND ONLINE-GAMING	BESTANDEN	NICHT BESTANDEN	K. A.	ANMERKUNGEN	METHODEN
	EXTERNE BEZUGNR.				VERWENDETE EINREICHUNG
ZUFALLSZAHLENGENERATOR					
Was das Design und die Implementierung betrifft, so muss sichergestellt werden, dass jeder Zufallszahlengenerator für Casino-Spiele mit einem Datensatz von mindestens 1.000.000 Ergebnissen einen der folgenden Tests erfolgreich besteht:	3.9.65				
der DIEHARD-Test (Marsaglia);	☒	☐	☐		
	3.9.65.a				
die NIST (National Institute of Standards and Technology) Statistical Test Suite; oder TESTU01	☒	☐	☐		
	3.9.65.b				
Bei mechanischen Zufallszahlengeneratoren wie Roulettekesseln ist es möglich, den Datensatz auf ein Minimum von 1000 Mal die möglichen Ergebnisse zu begrenzen. Erläuterung: Bei Verwendung eines physischen Würfels mit 6 möglichen Ergebnissen beträgt der Mindestdatensatz 6 * 1000 = 6000.	☐	☐	☒	Kein mechanisches RNG	
	3.9.65				

NIEDERLÄNDISCHE VORSCHRIFTEN UND ONLINE-GAMING	BESTANDEN	NICHT BESTANDEN	K. A.	ANMERKUNGEN	METHODEN
	EXTERNE BEZUGNR.				VERWENDETE EINREICHUNG
In Bezug auf Design und Implementierung muss sichergestellt werden, dass jeder Zufallszahlengenerator mit einer geeigneten Methode für Seeding und Re-Seeding ausgestattet ist, damit die Vorhersagbarkeit der Ergebnisse vermieden wird.	☒	☐	☐		
	3.9.66				
In Bezug auf Design und Implementierung, muss sichergestellt werden, dass alle Abweichungen in einem mechanischen Zufallszahlengenerator aufgezeichnet werden.	☒	☐	☐		
	3.9.78				

4. WEITERE INFORMATIONEN/FESTSTELLUNGEN.

k. A.

5. FAZIT.

Basierend auf den Testergebnissen[1,2] bestätigt BMM Spain Testlabs s. l. u., dass der zur Prüfung vorgelegte Artikel allen einschlägigen Vorschriften entspricht, die in Abschnitt „1“ dieses Berichts aufgeführt sind.

Mit freundlichen Grüßen

Piazza Lorenzo

Firmado digitalmente por Piazza Lorenzo
Fecha: 2023.08.14 09:12:27 +02'00'

Lorenzo Piazza

VP SD Landbased Italy and Eastern Europe

[1] Die in diesem Dokument enthaltenen Ergebnisse beziehen sich ausschließlich auf die getestete Stichprobe, wie sie im entsprechenden Abschnitt beschrieben ist.

[2] BMM Spain Testlabs s.l.u. übernimmt keine Haftung für die Ergebnisse, auf die in diesem Dokument verwiesen wird.