bmm testlabs

PROVNINGSRAPPORT

Jurisdiktion:	Sverige
Befogenhet:	Svensk spelande myndighet
Kund:	Eyecon Alderney Limited Inchalla, Le Val Alderney GY9 3UL
Tillverkare:	Eyecon Alderney Limited
Inlämningsreferens:	Inlämning mottagen 14 juni 2017 för projekt EYECON.1004
Utvärderad produkt:	Eyecon RNG
Utgivet av:	BMM Testlabs
Plats (er) för utvärdering:	BMM Testlabs Våning 3, 810 Whitehorse Road Box Hill, Victoria 3128 Australien
Projektnummer:	EYECON.1007
Rapportnummer:	EYECON.1007.01
Datum för utfärdande:	24 juni 2019
Datum för utvärdering:	27 maj 2019
Standarder testade:	SMFS 2018: 8 Spelbolagets föreskrifter och allmänna råd om tekniska krav och ackreditering av organ för inspektion, testning och certifiering av spelleverantörer
Intyg om överensstämmelse:	BMM intygar härmed att den Eyecon RNG uppfyller kraven ovan.
Underskrift:	
	Christopher Van Prooije, Senior Systems Consultant, Matematik **(Godkänd NATA-underskrift)**

NATA

NATA Accredited Laboratory Number: 15122
Godkänd för överensstämmelse med ISO / IEC 17025 - Testning

1. SYFTE:

Eyecon Alderney Limited har begärt BMM att utvärdera slumptalsgeneratorn (RNG) som användes för Eyecon RNG operationen iSverige.

2. UTVÄRDERINGSMETOD:

Utvärderingen utfördes med hjälp av BMM testprocedurer utformade för att säkerställa överensstämmelse med gällande tekniska standarder och ISO/IEC 17025.

De fullständiga detaljerna i testen lagras i kvalitetsledningssystemet.

3. BESKRIVNING AV RNG:

RNG använder en instans av den kryptografiskt säkra Java SecureRandom-klassen. Detta använder SHA-1 hash-algoritmen och ett 160-bitars tillstånd för att säkert generera slumpmässiga värden.

3.1 KÄLLKOD RECENSION:

Följande avsnitt beskriver implementeringen av RNG i källkoden. Lägg till och ta bort avsnitt efter behov.

3.1.1 Erbjuder

RNG är sådd med sina egna inre såddmekanismer, som bygger på flera hårdvaru- och programkällor för entropi, vilket gör att staten är helt oförutsägbar.

3.1.2 Oförutsägbarhet

RNG använder SHA-1 säker hash-algoritm som gör den oförutsägbar utan kännedom om den applicerade algoritmen, implementeringen och initialvärdena.

3.1.3 Skalning

Metoder tillhandahålls för att producera slumptal i målområdena i en likformig fördelning utan att införa någon förspänning.

3.1.4 Övervakning

En bildskärmstjänst kör test på nummer som dras från RNG en gång per minut för att upptäcka fel.

3.1.5 Trådsäkerhet

Genomförandet verifierades genom inspektion för att vara tråd säkert.

4. FILSIGNATURER:

Följande filer används av RNG.

Fil(er)	Typ*	Underskrift
eyecon-RNG-1.0.1.jar	SHA1	D2BFE8EF8FB4F0C33D2988F9A2A030FD66A295F9

5. TESTRESULTAT

Varje test testar hypotesen att RNG är en slumpmässig källkod. Ett "P-värde" produceras för varje testkörning, vilket är sannolikheten för att en verkligt slumpmässig process skulle ge samma eller ett extrema resultat. P-värdena förväntas vara jämnt fördelade mellan 0 och 1. Varje test utförs minst 100 gånger och P-värdena för varje test utvärderas med ett Anderson-Darling-test. Detta ger ett enda p-värde, vilket är sannolikheten för att de individuella P-värdena har producerats från en likformig fördelning.

Slutligen kombineras P-värdena från varje test i samma testpaket med användning av Holm-Bonferroni-metoden för att ge ett totalt P-värde. Denna process justerar varje P-värde för att säkerställa att den övergripande sannolikheten för att acceptera RNG som slumpmässigt matchar det konfidensintervall som används. Det totala p-värdet, som motsvarar det minsta av de justerade P-värdena, jämförs med ett specifikt alfa-värde för att bestämma om RNG accepteras eller avvisas som slumpmässigt för ett specifikt konfidensintervall. För ett 95 % konfidensintervall, är alfavärde använt 0.05. På liknande sätt är alfavärdet 0,01 för ett 99 % konfidensintervall. Både 95 % och 99 % konfidensintervaller beaktades för denna utvärdering.

Följande tabeller sammanfattar testresultaten. Se bilaga A för en beskrivning av de använda statistiska testerna.

5.1 EMPIRISKA TEST

Test	P-värdet	95 % konfidensinterva ll	99 % konfidensinterva ll
Frekvensanalys	1,000000	GODKÄND	GODKÄND
Autokorrelation	1,000000	GODKÄND	GODKÄND
Körtest	1,000000	GODKÄND	GODKÄND
Blanktest	1,000000	GODKÄND	GODKÄND
Kupongkollektortest	1,000000	GODKÄND	GODKÄND
Efterföljande test	0,762371	GODKÄND	GODKÄND
Pokertest	1,000000	GODKÄND	GODKÄND
Övergripande	**0,762371**	**GODKÄND**	**GODKÄND**

Slutsats: RNG **ACCEPTERAS** som slumpmässigt via 95 % konfidensintervallet.
Slutsats: RNG **ACCEPTERAS** som slumpmässigt vid 99 % konfidensintervallet.

5.2 DIEHARD TESTS

Test	P-värdet	95 % konfidensinterva ll	99 % konfidensinterva ll
Binary Rank 32x32 Test	1,000000	GODKÄND	GODKÄND
Binär Rank 6x8 Test	1,000000	GODKÄND	GODKÄND
Födelsedagsutrymmen Test	0,929823	GODKÄND	GODKÄND
Bitströmstest	0,969203	GODKÄND	GODKÄND
Räkna 1:ans strömtest	1,000000	GODKÄND	GODKÄND
Räkna 1:ans specifika test	1,000000	GODKÄND	GODKÄND
Körtest	1,000000	GODKÄND	GODKÄND
Krympningstest	1,000000	GODKÄND	GODKÄND
Övergripande	**0,929823**	**GODKÄND**	**GODKÄND**

Slutsats: RNG **ACCEPTERAS** som slumpmässigt via 95 % konfidensintervallet.
Slutsats: RNG **ACCEPTERAS** som slumpmässigt vid 99 % konfidensintervallet.

5.3 NIST-TESTER

Test	P-värdet	95 % konfidensinterva ll	99 % konfidensinterva ll
Ungefärligt Entropitest	1,000000	GODKÄND	GODKÄND
Blockfrekvensprov	1,000000	GODKÄND	GODKÄND
Kumulativ summatest	1,000000	GODKÄND	GODKÄND
Diskret Fourier Transform Test	1,000000	GODKÄND	GODKÄND
Frekvensanalys	1,000000	GODKÄND	GODKÄND
Linjärt komplexitetstest	1,000000	GODKÄND	GODKÄND
Längsta körning för en test	1,000000	GODKÄND	GODKÄND
Test för icke-överlappande mall-matchningar	1,000000	GODKÄND	GODKÄND
Överlappande mallmatchningstest	1,000000	GODKÄND	GODKÄND
Slumpmässigt utflyktstest	1,000000	GODKÄND	GODKÄND
Slumpmässigt utflyktsvarianttest	1,000000	GODKÄND	GODKÄND
Ranktest	1,000000	GODKÄND	GODKÄND
Körtest	1,000000	GODKÄND	GODKÄND
Serie	1,000000	GODKÄND	GODKÄND
Universellt test	1,000000	GODKÄND	GODKÄND
Övergripande	**1,000000**	**GODKÄND**	**GODKÄND**

Slutsats: RNG **ACCEPTERAS** som slumpmässigt via 95 % konfidensintervallet.
Slutsats: RNG **ACCEPTERAS** som slumpmässigt vid 99 % konfidensintervallet.

6. AVVIKELSER:

Inga.

7. VILLKOR:

Inga.

8. YTTERLIGARE INFORMATION:

Inga.

9. SAMMANFATTNING

Som ett resultat av statistisk testning och källkodsbedömning anser BMM att den Eyecon RNG tillhandahåller enhetligt slumpmässiga data som är lämpliga för sin avsedda tillämpning. Denna RNG uppfyller gällande krav för drift i Sverige.

10. VILLKOR OCH BESTÄMMELSER:

BMM Testlabs ("BMM") har genomfört en testnivå av spelprodukten som historiskt sett varit tillräcklig för en inlämning av denna typ. Emellertid är det oundvikligt att man inte kan verifiera effekterna av alla möjliga konfigurationer och miljöer som förekommer i de faktiska spelplatserna, som är inbyggda i testning i en laboratoriemiljö.

Denna testrapport används av kunden för jurisdiktion ("jurisdiktion") som hänvisas till i rapporten ("Rapporten") och verifierar endast, från det angivna datumet, den spelprodukt som beskrivs i rapporten underställda några villkor eller begränsningar anges däri.

Tillverkaren som nämns i rapporten är ensam ansvarig för innehav av lämplig licens för att sälja, hyra ut, tillhandahålla tjänster eller tillhandahålla spelleveranser eller spelrelaterade tjänster inom jurisdiktionen och för att de behöriga myndigheternas pågående krav uppfylls. Det är tillverkarens och operatörens ansvar att se till att spelprodukten som beskrivs i denna rapport installeras, underhålls och drivs korrekt utan defekter och säkert i enlighet med behörighetskraven.

Rapporten och testningen utförd av BMM är proprietär till BMM. Denna rapport utfärdas enbart till förmån för kunden och får inte reproduceras, återges, eller överlämnas helt eller delvis till någon part som inte nämns i rapporten utan skriftligt godkännande av BMM, med undantag av en behörig myndighet i jurisdiktion. Ingen tredje part får använda, förlita sig eller hänvisa till rapporten, dess innehåll eller något relaterat dokument utan skriftligt tillstånd från BMM. Om BMM beviljar samtycke skickar BMM denna rapport via e-post enligt anvisningarna. BMM vidtar försiktighetsåtgärder för att säkra PDF-dokumentet, men BMM skickar inte e-postmeddelandet via någon krypterad metodik.

Undertecknade intygar att straffavvikelsen i enlighet med kraven i behörigheten och att spelprodukten uppfyller kraven i dess lagar och de förordningar som antagits härmed, samt alla publicerade tekniska standarder, kontrollstandarder, kontrollförfaranden, policyer, branschmeddelanden och liknande krav som genomförts eller utfärdats av behörigheten till det bästa av BMM: s kunskaper och övertygelse.

Trots ovanstående kan någon regulator skriva ut, reproducera och överföra något dokument eller information till någon part som regulatorn, enligt eget gottfinnande, anser lämpligt.

BMM GÖR INTE, OCH UTTRYCKER INTE, ALLA ANDRA GARANTIER AV NÅGOT AVSLUT, UTTRYCKLIGT ELLER UNDERFÖRSTÅTT, INKLUSIVE OCH UTAN BEGRÄNSNING AV GARANTI FÖR ICKE INTRÄDANDE, SÄLJBARHET, GODKÄNNANDE ELLER EGENHET FÖR NÅGOT SÄRSKILT SYFTE. ANSVAR FÖR SKULDER OCH SKYLDIGHETER OCH RÄTTIGHETER FÖR MOTTAGAREN, UNDER ELLER I FÖRBINDELSE MED DETTA AVTAL, SKALL BEGRÄNSAS AV MOMSTYP, BYTE AV TJÄNSTER SOM SKICKAS ELLER RÄDDNING AV BMM AV PENGAR SOM MOTTAS AV DENNE FÖR TILLHANDHÅLLNA TJÄNSTER. INGA EVENTUELLA SKADOR SKAL BMM GÖRAS ANSVARIGA FÖR VAD SOM GÄLLER KUNDEN ELLER NÅGON TREDJE PART FÖR EVENTUELLA, OAVSIKTLIGA, DIREKTA, INDIREKTA ELLER SÄRSKILDA SKADOR, INKLUSIVE UTAN BEGRÄNSNING AV SKADOR FÖR TILLGÄNGLIGA RESULTAT ELLER INKOMSTER, AFFÄRSBESKRIVNING ELLER STRAFFBELAGDA SKADOR, SJÄLVA OM BMM VAR FÅTT RÅD OM MÖJLIGHETEN FÖR SÅDANA SKADOR.

APPENDIX A. HYPOTESPRÖVNING

Följande tester användes för att testa de statistiska egenskaperna hos RNG.

A1. EMPIRISKA TEST

De empiriska testen är baserade på de testerna som beskrivits av Donald Knuth i The Art of Computer Programming Volume 2: Seminumerical Algorithms (1968, reviderad i 1997). De testar sekvenser av tal som skalas till specifika områden.

Frekvensanalys	Antalet tal för varje tal som förekommer över provet.
Autokorrelation	Antalet icke-överlappande grupper av tal som uppträder tillsammans. Gruppstorlekar på två, tre och fyra testas separat.
Körtest	Antalet stigande och nedåtgående sekvenser av siffror. Observera att detta är ett annat test för körtestet i Diehard och NIST-testen.
Blanktest	Antalet storlekar av luckor mellan successiva förekomster av ett givet antal. Varje nummer i intervallet testas separat.
Kupongkollektortest	Antal sekvenslängder som krävs för att slutföra en fullständig uppsättning av varje nummer inom intervallet.
Efterföljande test	Liknande Serial Correlation Test för nummerpar, utom att titta på siffror åtskilda av ett visst glapp. Stegstorlekarna 5, 10, 15 och 20 testas separat.
Pokertest	Sekvensen är uppdelad i grupper om fem. Antalet unika värden i varje grupp räknas.

A2. DIEHARD TESTS

Diehard-testen är baserade på testpaketet som publicerades av George Marsaglia 1995. De testar sekvenser av rå binär utgång från RNG.

Binary Rank 32x32 Test	Matriser skapas med 32 32-bitars ord. Räkningarna av de resulterande matriserna räknas.
Binär Rank 6x8 Test	Samma som det binära klass 32x32-testet, förutom att varje matris bildas med 6 värden, var och en tar 8 bitar från successiva 32-bitars ord med en specifik förskjutning. Alla möjliga förskjutningar testas separat.
Födelsedagsutrymmen Test	26-bitars värden tas från successiva 32-bitars ord med en specifik förskjutning. Värdena sorteras och avståndet mellan dem beräknas. Antalet avstånd av samma storlek räknas. Alla möjliga förskjutningar testas separat.
Bitströmstest	Block av 2 ^ 18 värden behandlas som en ström av överlappande 20-bitars värden. Antalet möjliga 20-bitars värden som inte hittas i varje block räknas.
Räkna 1:ans strömtest	8-bitars värden tas och tilldelas ett "brev" baserat på antalet som visas i binär representation av varje värde. Överlappande grupper med 5 "bokstäver" räknas.
Räkna 1:ans specifika test	I likhet med greven 1:ans strömtest, utom 8 bitars värden tas från successiva 32-bitars ord med en specifik förskjutning. Alla möjliga förskjutningar testas separat.
Körtest	Räknar sekvenser för att öka och minska 32-bitars ord. Observera att detta är ett annat test för körtestet i empiriska och NIST-testen.
Krympningstest	Ett värde på 2 ^ 31 multipliceras upprepade gånger med 32-bitars ord dividerande med 2 ^ 32 och tar taket för resultatet varje gång. Antalet på varandra följande ord som krävs för att sänka värdet ner till 1 räknas. Värdet återställs till 2 ^ 31 och processen upprepas.

A3. NIST-TESTER

NIST-testen är baserade på testserien som släpptes av National Institute of Standards and Technology i specialpublikation 800-22, Revision 1a (reviderad april 2010). De testar sekvenser av rå binär utgång från RNG.

Ungefärligt Entropitest	I likhet med Serietestet räknas varje m-bitvärde, utom det gör det för två intilliggande m-bitlängder och jämför de två.
Blockfrekvensprov	I likhet med Frekvensprovet delas uppgifterna in i lika stora block. Antalet och nollor i varje block räknas.
Kumulativ summatest	Slumpmässiga promenader skapas genom att konvertera data till +1 / -1 för 1/0 respektive summera konsekutiva värden.
Diskret Fourier Transform Test	Data transformeras med användning av en diskret Fourier-transform. Antalet toppar inom 95 % tröskeln räknas.
Frekvensanalys	Antalet ettor och nollor i binärutmatningen räknas.
Linjärt komplexitetstest	Längden på den linjära komplexiteten hos den slumpmässiga sekvensen bestäms.
Längsta körning för en test	Uppgifterna delas in i lika stora block. Den längsta loppet av de i varje block bestäms och räknas.
Test för icke-överlappande mall-matchningar	Uppgifterna delas in i lika stora block. Varje block söker efter ett specifikt bitmönster och räknas. Ett separat test körs för olika bitmönster. Varje bitmönster som söks överlappar inte med sig själv. Det vill säga när mönstret matchas kan slutet på mönstret inte vara starten på en annan match.
Överlappande mallmatchningstest	I likhet med Testet för icke-överlappande mall-matchning, är det bara att söka ett mönster som kan överlappa med sig själv.
Slumpmässigt utflyktstest	Som med det kumulativa summan testet. ,slumpmässiga promenader skapas genom att konvertera data till +1 / -1 för 1/0 respektive summera konsekutiva värden. Antalet gånger ett visst tillstånd besöks mellan retur till noll räknas. Separata test körs för olika tillstånd från -4 till +4, inte inklusive 0.
Slumpmässigt utflyktsvarianttest	I likhet med det slumpmässiga utflyktstestet, räknat för det antal gånger det givna tillståndet är besökt, räknas det för hela sekvensen. Separata test körs för olika tillstånd från -9 till +9, inte inklusive 0.
Ranktest	Matriser skapas med 32 32-bitars ord. Räkningarna av de resulterande matriserna räknas. Observera att det här är i grunden samma test som Binary Rank 32x32-testet i Diehard-testen, även om implementeringen kan skilja sig åt.
Körtest	Körningar av på varandra följande bitar av samma värde av olika längder räknas.
Serie	Antalet möjliga m-bitvärden. Separata test körs för olika m-bitlängder.
Universellt test	Avstånd mellan upprepade bitmönster räknas.

--- SLUT PÅ RAPPORT ---