Gambling Commission
approved Test House
Accredited to
ISO/IEC 17025:2005

NMi Metrology & Gaming Ltd
Parc Menai
Bangor
Gwynedd LL57 4EZ
United Kingdom
Tel: +44 (0)1248 660550
http://www.nmi.uk.com

UKAS
TESTING
4403

Report to NEKTAN

NEKTAN RNG

Report Reference ID	Jurisdiction	Issue Date
NMI/128/015/UK/RTS/01	United Kingdom	29/04/2015

Executive Summary

This report summarises the testing of NEKTAN's 'SecureRandom' Random Number Generator (RNG).

The software RNG (identified as v1.10) is currently deployed into the following platform baseline:

- Platform Supplier: NEKTAN
- Platform Version: 5.25

The scope of the testing was the RNG algorithm only. NEKTAN provided source code and a test harness for empirical testing. The containing platform was not supplied. Our assessment methods included statistical analysis of the RNG outputs and source code review.

The RNG has been assessed for compliance with section 7A of the "Remote gambling and software technical standards" (August 2009, updated October 2014) and our methodology complies with "Level 1" as defined in the "Testing strategy for compliance with remote gambling and software technical standards" (first published August 2009, updated October 2014).

In order to assess the suitability of the RNG for the purpose of supplying data to games, data for the following representative ranges were drawn:

- 0 - 36 (for Roulette games)
- 0 - 51 (for single card deck outcomes)
- 0 - 127 (for slot game outcomes)

The RNG outputs were determined to be acceptably random, unpredictable (even with full knowledge of the system) and not reproducible.

No issues are raised in respect of the applicable requirements assessed.

A B Hughes

Aled Hughes
Laboratory Manager

Disclaimer
This report and any accompanying documents are provided 'as is' with no warranties. All systems may contain defects and nothing in this document is intended to represent or warrant that any items assessed are complete and free from errors. The operator remains solely responsible for the design, functionality and provision of their product(s) and service(s), including any liability arising from legal infringement, technical non-compliance or product warranty. This document remains the property of NMi Metrology & Gaming Ltd and, apart from supply to the intended regulator, is not to be copied, shared or distributed in any way without the express consent of NMi Metrology & Gaming Ltd.

Table of Contents

Introduction

NMi Metrology & Gaming Ltd ("NMi UK") is fully approved by the UK Gambling Commission and accredited to ISO/IEC 17025:2005 (by the United Kingdom Accreditation Service, UKAS) to undertake compliance testing of all categories of modern gaming systems and related equipment at their own and their customer's premises. NMi UK's ISO 17025 accreditation schedule is downloadable from the UKAS website. The Gambling Commission's list of approved Test Houses is published on their website.

Scope of ISO/IEC 17025:2005

NMi UK's ISO/IEC 17025:2005 accreditation includes the testing of terrestrial and remote gaming systems for compliance with the Gambling Commission's applicable Technical Standards and the Gaming Machine (Circumstances of Use) Regulations 2007 (Statutory Instrument No. 2319) of the Gaming Act (commonly known as the "Section 240" regulations). All assessments in the following sections of this report are provided under ISO/IEC 17025:2005 except (as in the case of interpretations, opinions and suggestions) where otherwise stated.

Caveats

The results presented in this document are a summary of the testing work undertaken, and this report is subject to a number of caveats, including:

- All items provided for inspection and/or testing are declared by the customer to be configured identically to those in commercial use, with the exception of operator-configurable aspects that will not have a bearing on game fairness or player returns.
- Game software and/or source code provided for simulation, empirical testing, analysis and/or review is declared by the customer to behave identically to the software and/or code in commercial use.
- The decisions taken by the supplied simulator(s) are declared by the customer to be accurate emulations of those that would be expected to be taken by real players.

All efforts have been taken to ensure that the testing undertaken has been as exhaustive as necessary to demonstrate compliance or non-compliance. NMi UK takes on trust that all submissions (including all hardware, software and documentation) and all communications are accurate, truthful, and that there is no intention to deceive or subvert the assessment of compliance.

Quality Control

The monitoring of this testing project was the responsibility of the management of NMi UK and every effort has been made to ensure the accuracy of the information contained in this report. If errors or omissions are discovered, please contact us with details as soon as possible. NMi UK reserves the right to revise and reissue this report if additional information is presented or discovered.

References

1. Our accreditation schedule is available via the 'View Full Schedule (PDF)' links on the following web pages: http://www.ukas.org/testing/lab_detail.asp?lab_id=2749 and http://www.ukas.org/testing/lab_detail.asp?lab_id=2750
2. The list of Gambling Commission approved Test Houses is available via the 'Test Houses approved' link on the following web page: http://www.gamblingcommission.gov.uk/shared_content_areas/test_houses.aspx

Test Item Details

Critical Components

SHA-1 checksum	File name
2217639a347a5d72004a732abd093bff3a0f944e	RNGDistribution.class

Testing Overview

Customer Contacts

The customer liaisons were Jane Ryan, James Bloom and Matthew Mitchell.

Dates

Testing was undertaken during the following periods:

- 22/04/2015 - 28/04/2015

Locations

Testing was undertaken at the following locations:

- NMi UK, 1-3 Llys Helyg, Parc Menai, Bangor LL57 4EZ, UK.
- NMi, 530 - 4445 Lougheed Highway, Burnaby, British Columbia, V5C 0E4, Canada

Applicable Standards

Conformance with the following standards has been assessed, under the terms of NMi UK's ISO/IEC 17025:2005 accreditation:

Document	Abbreviation Used
Remote Gambling and Software Technical Standards (August 2009, Updated October 2014)	UK_RTS

Methods

Our assessment methods included statistical analysis of the RNG outputs and source code review.

RNG Analysis

Source code & dependencies

The RNG submission consisted of a virtual machine (VM) and a single Java file containing an implementation of Java's `SecureRandom` class (`java.security.SecureRandom`), running under Java 1.8.0_11 (JDK 8).

SecureRandom is generally-accepted to be cryptographically-secure provided (a) it is configured correctly, and (b) sufficient system entropy is available for its operation. In this implementation it opens channels to `/dev/random/` and `/dev/urandom`; the former blocks if insufficient system entropy is available, the latter does not.

Under normal operating conditions in which sufficient system entropy is available, the outputs will be unpredictable without complete knowledge of the algorithm, its implementation, and the underlying system state.

Empirical testing results

Degrees of freedom

The following samples were generated:

- 3 sets of 3 million raw number between 0 and 2^32 - 1 (inclusive)
- 1 set of 60 million raw number between 0 and 2^32 - 1 (inclusive)
- 1 set of 60 million integers between 0 and 36 (inclusive)
- 1 set of 60 million integers between 0 and 51 (inclusive)
- 1 set of 60 million integers between 0 and 127 (inclusive)

Tests under high load, with insufficient system entropy

Under high load, with limited system entropy available, failure patterns were detected.

Tests under high load, with sufficient system entropy

Under high load, with sufficient system entropy available, no failures were detected. The results can be summarised as follows:

Analysis of 3 sets of 3 million unscaled 32-bit raw numbers

The numbers passed the Diehard Battery of tests, confirming that the software RNG is functioning correctly from a bitwise randomness perspective.

Analysis of 1 set of 60 million unscaled 32-bit raw number

The numbers passed the NIST Battery of tests, confirming that the software RNG is functioning correctly from a bitwise randomness perspective.

Analysis of 60 million scaled integers between 0 and 36 (inclusive)

The frequency of occurrences of the possible outcomes was as expected for a random distribution. The outcomes covered the full range of possibilities. No pairwise correlations were observed outside of the expectations for a random sample. No regular patterns or groupings were observed. The gaps between repetitions of outcomes were observed to be random.

Analysis of 60 million scaled integers between 0 and 51 (inclusive)

The frequency of occurrences of the possible outcomes was as expected for a random distribution. The outcomes covered the full range of possibilities. No pairwise correlations were observed outside of the expectations for a random sample. No regular patterns or groupings were observed. The gaps between repetitions of outcomes were observed to be random.

Analysis of 60 million scaled integers between 0 and 127 (inclusive)

The frequency of occurrences of the possible outcomes was as expected for a random distribution. The outcomes covered the full range of possibilities. No pairwise correlations were observed outside of the expectations for a random sample. No regular patterns or groupings were observed. The gaps between repetitions of outcomes were observed to be random.

Conclusions

Under high load, with limited system entropy available, failure patterns were detected, and therefore we recommend that the entropy of the containing system be monitored as a preventative measure.

Under normal operating conditions in which sufficient system entropy was available, the RNG outputs were determined to be acceptably random, unpredictable (even with full knowledge of the system and initial system state) and not reproducible.

Appendix A: Requirements Met

Reference:	UK_RTS / RTS - 7 Generation of random outcomes (7, 7A.1)
Requirement: To ensure that games and other virtual events operate fairly. Random number generation and game results must be 'acceptably random'. Acceptably random here means that it is possible to demonstrate to a high degree of confidence that the output of the RNG, game, lottery and virtual event outcomes are random, through, for example, statistical analysis using generally accepted tests and methods of analysis. Adaptive behaviour (i.e. a compensated game) is not permitted.	
Assessment: The RNG was determined to be acceptably random, unpredictable, and not reproducible for all of the ranges assessed. No evidence of compensatory or adaptive behaviour was observed in the RNG source code supplied.	

Reference:	UK_RTS / RTS - 7 Generation of random outcomes (7A.3, 7A.4, 7A.5, 7A.6, 7A.7, 7A.8)
Requirement: a. RNG's should be capable of demonstrating the following qualities: i. the output from the RNG is uniformly distributed over the entire output range and game, lottery, or virtual event outcomes are distributed in accordance with the expected/theoretical probabilities ii. the output of the RNG, game, lottery, and virtual event outcomes should be unpredictable, for example, for a software RNG it should be computationally infeasible to predict what the next number will be without complete knowledge of the algorithm and seed value iii. random number generation does not reproduce the same output stream (cycle), and that two instances of a RNG do not produce the same stream as each other (synchronise) iv. any forms of seeding and re-seeding used do not introduce predictability v. any scaling applied to the output of the random number generator maintains the qualities above.	
Assessment: The RNG was determined to be acceptably random, unpredictable, and not reproducible for all of the ranges assessed. No evidence of compensatory or adaptive behaviour was observed in the RNG source code supplied.	

Appendix B: Requirements Not Applicable

Reference: UK_RTS / RTS - 7 Generation of random outcomes (7, 7A.2)

Requirement:

To ensure that games and other virtual events operate fairly.

Where lotteries use the outcome of other events external to the lottery, to determine the result of the lottery (for example, using numbers from the National Lottery) the outcome must be unpredictable and externally verifiable.

Assessment:

This was a test of the software RNG only. The submission does not constitute a lottery game.

Reference: UK_RTS / RTS - 7 Generation of random outcomes (7A.9, 7A.10, 7A.11, 7A.12)

Requirement:

b. For lotteries using external events - where it is not practical to demonstrate 7a. - the events outcomes should be:

i. unpredictable, that is, events should be selected only where they may reasonably be assumed to be random events

ii. unable to be influenced by the lottery operator (or external lottery manager)

iii. publicly available and externally verifiable, for example, events that are published in local or national press would be acceptable.

Assessment:

This was a test of the software RNG only. The submission does not constitute a lottery game.

Reference: UK_RTS / RTS - 7 Generation of random outcomes (7A.13, 7A.14, 7A.15, 7A.16)

Requirement:

c. For games or virtual events that use the laws of physics to generate the outcome of the game (mechanical RNGs), the mechanical RNG used should be capable of meeting the requirements in a. where applicable and in addition:

i. the mechanical pieces should be constructed of materials to prevent decomposition of any component over time (e.g. a ball shall not disintegrate)

ii. the properties of physical items used to choose the selection should not be altered

iii. players should not have the ability to interact with, come into physical contact with, or manipulate the mechanics of the game.

Assessment:

This was a test of the software RNG only.

Reference: UK_RTS / RTS - 7 Generation of random outcomes (7A.13, 7A.17)

Requirement:

c. For games or virtual events that use the laws of physics to generate the outcome of the game (mechanical RNGs), the mechanical RNG used should be capable of meeting the requirements in a. where applicable and in addition:

d. Restricting adaptive behaviour prohibits automatic or manual interventions that change the probabilities of game outcomes occurring during play. Restricting adaptive behaviour is not intended to prevent games from offering bonus or special features that implement a different set of rules, if they are based on the occurrence of random events.

Assessment:

This was a test of a random outcome generator, and the submission did not include any specific game code or customer interfaces.

END OF REPORT