Test report

Product name	: Random Number Generator (RNG)
Jurisdiction	: United Kingdom
Applicant	: Skywind Holdings Limited
Test institute	: Trisigma B.V.
Type of product	: Random Number Generator

Author: M. Hoogma

Authorised by: Ing. R. Hubregtse 01-12-2017
Quality Manager

Copyright © Trisigma B.V., Geldermalsen, the Netherlands. All rights reserved. The contents of this report may only be transmitted to third parties in its entirety. Application of the copyright notice and disclaimer is compulsory.

Trisigma B.V. disclaim liability for any direct, indirect, consequential or incidental damages that may result from the use of the information or data, or from the inability to use the information or data.

Trisigma B.V.
Rijnstraat 30
4191 CL Geldermalsen
The Netherlands
www.trisigma.nl

TABLE OF CONTENTS

1. TEST INSTITUTE

Trisigma B.V. (here after Trisigma) provides compliance and type approval services to the gaming industry and authorities. The Trisigma test labs are located in The Netherlands and have extensive facilities for testing and approval of online and land based gaming systems. Trisigma has been accredited by the Dutch Council of Accreditation for both standards ISO/IEC 17020 (with identification I254) and ISO/IEC 17025 (with identification L531) within the scope of compliance testing and examination of gaming systems. It is Trisigma's policy to carry out all activities according to these high quality standards in order to assure the international recognition of Trisigma certifications, reports and declarations.

This report presents the Trisigma final conclusion of compliance, the scope of examination, the specific identification of the gaming system and an overview of the applicable requirements including the appraisal with regard to the gaming system under examination.

This report has been constructed under the supervision and responsibility of Trisigma's Quality Manager. Every effort has been made to ensure the quality and accuracy of the information contained in this report. If errors or omissions are discovered, please contact us with details. Trisigma B.V. reserves the right to issue revisions of this test report if additional information is presented or discovered.

2. TEST METHODS

Trisigma examines gaming systems using accredited and recognized assessment methods. These methods cover all applicable components and characteristics of the product under examination.

Qualified test engineers carry out a comprehensive compilation of test methods using documentation review, measurements, evaluation of calculations and simulations, statistical tests, functional tests, visual assessment and source code analyses and supervised builds in order to examine the product from a requirements point of view. These test methods comprises the functional and statistical behavior of the gaming system.

3. GENERAL REPORT DATA

Report number	3s.17.784_UK.R1
Jurisdiction	United Kingdom
Requirements	Remote gambling and software technical standards June 2017
Additional regulations or directions	Testing strategy for compliance with remote gambling and software technical standards, June 2017.
Test period	November 2017
Project Engineer	M. Hoogma
Revision information	This revision R1 supersedes the previous version 3s.17.234_UK.R0. R1 aims at confirming compliance of the test item(s) against the updated UKGC's Remote gambling and software technical standards, June 2017 upon request of the applicant. Test item(s) remain those listed and verified by previous R0 revision.
References	-

4. APPLICANT DATA

Company name	Skywind Holdings Limited
Address	Unit 2W - Second Floor Quay House, South Quay Douglas IM1 5AR Isle of Man
Contact	Mr Uri Cohen

5. CONCLUSION AND RECOMMENDATION

The Random Number Generator (RNG) complies with the United Kingdom Remote gambling and software technical standards.

It is the recommendation of Trisigma that the RNG be approved for use in the jurisdiction of the United Kingdom.

The RNG has been tested according with the procedure for testing of the Testing strategy for compliance with remote gambling and software technical standards, June 2017.

6. PLATFORM INFORMATION

Supplier	Skywind Falcon
Version	1.0.1

7. REQUIREMENTS – TEST RESULTS OVERVIEW

Requirements within this scope are included in this test results overview.

Test results overview		
Article	**Requirement Text**	**Verdict**
RTS requirement 7A	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.	**PASS**
	Remarks/Findings: Research demonstrates that events of chance are statistically random.	
RTS requirement 7A (continued)	Where lotteries use the outcome of other events external to the lottery, to determine the result of the lottery the outcome must be unpredictable and externally verifiable.	**Not Applicable**
	Remarks/Findings: This is not a lottery game.	
RTS implementation guidance 7A a.	RNG's should be capable of demonstrating the following qualities:	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A a. 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	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A a. 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	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A a. 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)	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A a. iv.	any forms of seeding and re-seeding used do not introduce predictability	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A a. v.	any scaling applied to the output of the random number generator maintains the qualities above.	
	Remarks/Findings: This is an explanatory text only.	

RTS implementation guidance 7A b.	For lotteries using external events - where it is not practical to demonstrate 7a. - the events outcomes should be:	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A b. i.	unpredictable, that is, events should be selected only where they may reasonably be assumed to be random events	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A b. ii.	unable to be influenced by the lottery operator (or external lottery manager)	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A b. iii.	publicly available and externally verifiable, for example, events that are published in local or national press would be acceptable.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A 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:	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A c. i.	the mechanical pieces should be constructed of materials to prevent decomposition of any component over time (e.g. a ball shall not disintegrate)	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A c. ii.	the properties of physical items used to choose the selection should not be altered	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A c. iii.	players should not have the ability to interact with, come into physical contact with, or manipulate the mechanics of the game.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7A 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.	
	Remarks/Findings: This is an explanatory text only.	
RTS requirement 7B	As far as is reasonably possible, games and events must be implemented fairly and in accordance with the rules and prevailing payouts, where applicable, as they are described to the customer.	**PASS**
	Remarks/Findings: The RNG and mapping and scaling is implemented fairly.	
RTS implementation guidance 7B a.	Games should implement the rules as described in the rules available to the customer before play commenced.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7B b.	The mapping of the random inputs to game outcomes should be in accordance with prevailing probabilities, pay tables, etc.	
	Remarks/Findings: This is an explanatory text only.	

RTS implementation guidance 7B c.	When random numbers, scaled or otherwise, are received, e.g. following a game requesting a sequence of random numbers, they are to be used in the order in which they are received. For example, they may not be discarded due to adaptive behaviour.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7B d.	Numbers or sequences of numbers are not to be discarded, unless they fall outside the expected range of numbers required by the virtual event – such an occurrence should result in an error being logged and investigated.	
	Remarks/Findings: This is an explanatory text only.	
RTS requirement 7C	Game designs or features that may reasonably be expected to mislead the customer about the likelihood of particular results occurring are not permitted, including substituting losing events with near-miss losing events and simulations of real devices that do not simulate the real probabilities of the device.	**Not Applicable**
	Remarks/Findings: Game implementation is outside the scope of this test report.	
RTS implementation guidance 7C a.	Where a virtual event simulates a physical device, the theoretical game probabilities should match the probabilities of the real device (for example, the probability of a coin landing heads must be 0.5 every time the coin is tossed).	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7C b.	Where multiple physical devices are simulated the probabilities of each outcome should be independent of the other simulated devices.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7C c.	Games may not falsely display near-miss results, that is, the event may not substitute one losing outcome with a different losing outcome.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7C d.	Where the event requires a pre-determined layout (for example, hidden prizes on a map), the locations of the winning spots should not change during play, except as provided for in the rules of the game.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7C e.	Where games involve an element of skill, every outcome described in the virtual event rules or artwork should be possible, that is, the customer should have some chance of achieving an advertised outcome regardless of skill.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7C f.	Where a customer contributes to a jackpot pool, that customer should be eligible to win the jackpot whilst they are playing that game, in accordance with the game and jackpot rules.	
	Remarks/Findings: This is an explanatory text only.	
RTS requirement 7D	The rules, payouts and outcome probabilities of a virtual event or game may not be changed while it is available for gambling, except as provided for in the rules of the game, lottery or virtual event. Such changes must be brought to customer's attention.	**Not Applicable**
	Remarks/Findings: Game implementation and external RNG usage is outside the scope of this test report.	

RTS implementation guidance 7D a.	Changes to game or event rules, paytables or other parameters that change the way in which a game, lottery, or event works, the winnings paid, or likelihood of winning (except as described in 7Dc), should be conducted with the game or event taken offline or suspended.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D b.	Altered games, lotteries, and events should display a notice that informs customers that the game or event has been changed, for example, 'rules changed', 'new odds', or 'different payouts'. The notice should be displayed on game selection screens and on the events themselves if it is possible for the customer to go straight to the event without using a selection screen.	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D c.	This requirement is not intended to prevent games and virtual events where specified changes occur legitimately, in accordance with the game or event rules, for example:	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D c. i.	virtual events, such as virtual racing products where the odds differ from event to event depending on the virtual runners	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D c. ii.	virtual games, such as bingo where the odds of winning are dependent on the number of entrants	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D c. iii.	games with progressive jackpots, where the amount that can be won changes over time	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D c. iv.	games with bonus rounds where different rules apply, so long as these rounds are properly described to the customer	
	Remarks/Findings: This is an explanatory text only.	
RTS implementation guidance 7D c. v.	unspecified changes to rules, paytables or other parameters that change the way in which a game, lottery or event works are not permitted, for example, rules that state 'game rules may be changed at any time' would not be acceptable.	
	Remarks/Findings: This is an explanatory text only.	
RTS requirement 7E	Except in the case of subscription lotteries, the system clearly and accurately display the result of the game or event and the customer's gamble.	**Not Applicable**
	Remarks/Findings: Game presentation is outside the scope of this test report.	
RTS requirement 7E (continued)	The result must be displayed for a length of time that may reasonably be expected to be sufficient for the customer to understand the result of the game or event in the context of their gamble.	**Not Applicable**
	Remarks/Findings: Game presentation is outside the scope of this test report.	
RTS implementation guidance 7E	The game artwork and text should be sufficient to provide the customer with all of the information required to determine whether they have lost or won, and the value of any winnings.	
	Remarks/Findings: This is an explanatory text only.	

APPENDIX A: RNG details and scope and approach to testing

The RNG is a wrapper around a standard JavaScript Mersenne Twister implementation.

RTS requirement 7A

The requirement to have unpredictable sequences of data for a software random number generator means that it is possible to demonstrate to a high degree of confidence that the output of the RNG resulting from a known algorithm is random, through, for example, statistical analysis using generally accepted tests and methods of analysis therefore to produce 'acceptably random' sequences. Adaptive behaviour (i.e. a compensated game) is not permitted.

The standards document also provides several guidelines as to the methods that are to be used to evaluate the random number generators:

RTS implementation guidance 7A

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.

In the remainder of this document, these requirements are demonstrated by a statistical analysis of the output of the random number generator and an inspection of the source code.

RNG implementation

The RNG is a wrapper around the well-known Mersenne Twister algorithm, specifically the JavaScript MersenneTwister() base function version 1.1.0. Further technical details available at https://www.npmjs.com/package/mersenne-twister.
All game servers on the Skywind Falcon platform run an instance of this MersenneTwister() function. Each time a client needs a random number it connects to a game server and gets one.

The wrapper file 'random.ts' contains also a secondary RNG which was not required to be included within the testing scope. As a consequence, this report doesn't include conclusions nor recommendation with regards to the aforementioned RNG which, in absence of proper testing against the referenced standards, shall be used to support operations not directly affecting any game logic.

Statistical analysis

In order to verify that the pseudo random numbers generated by the algorithm satisfy the 'acceptably random' requirement, the output of the RNG is subjected to a statistical analysis. This analysis consists of a series of tests that determine the chance that these numbers have not been generated by a random-like process. Each of these tests observes the behaviour of a specific aspect of the series of random numbers, and will fail if the chance that a random process has not generated these series is above a certain threshold. These tests will verify whether the output from the RNG is uniformly distributed among the entire output range as stipulated by guidance rule 7A a. i), but is not limited to just this verification.

For statistical analysis of the output of the random number generator a file was created containing 3 billion 32 bit random numbers generated by the RNG. For this generation a test setup was used with an identical configuration as used in the production environment.

The software used for statistical analysis is the Dieharder RNG test suite (Brown, 2015). This is a test suite maintained by Robert G. Brown from Duke University Physics Department. It builds upon the Diehard battery of tests from George Marsaglia (Marsaglia, 1995), but also includes tests from the statistical test suite from NIST (Soto, 1999) and tests developed by Robert G. Brown himself.

Results of the statistical analysis

The complete Dieharder suite was run using a sample of 3 billion random numbers generated with a platform that was similar to the production platform. The test suite consists of independent tests. For each test random numbers from the sample were used. Because the entire suite needs more than 3 billion random numbers, reuse of the random numbers from the data file was allowed, but not in the same test.

The results of all the tests are listed in appendix B.

All tests passed the first assessment.

Source code inspection

The source code was inspected to verify that the remaining requirements ii) - v) have been met. In this section for each of the requirements a brief outline is given how the source code ensures that the requirements are met.

The RNG is unpredictable

The Mersenne Twister algorithm produces 32-bit word length numbers. The cycle length is a very long period of 2^{19937} – 1. The test results show the RNG to be unpredictable random. Each client receives a random number from a game server out of a pool of ten game servers. This provides protection against prediction and backtracking attacks on the RNG.

The seeding is unpredictable

The Mersenne Twister implementation is designed to seed itself at initialisation, the RNG will be seeded with a source of entropy from the underlying operating system. There is no subsequent reseeding. The game servers are restarted every two weeks (after patching).

The reseeding will in practice comply with the implementation guidance 7A. a. iv.

The RNG does not cycle or synchronize

The Mersenne Twister implementation has 2^{19937} – 1 internal states. The wrapper code will re-seed with each restart of the game server, as demonstrated in the previous section. This will ensure that the RNG will not cycle and does not synchronize.

Synchronization is prevented by not explicitly seeding the algorithm. Every instance will seed itself using entropy from the underlying operating system.

Scaling is applied properly

Scaling is performed within the MersenneTwister() function, which yields a real number in the range [0,1). Further scaling is performed in the wrapper.

No other functions are present to alter the results of the random number generator algorithm.

Limitations

- **Acceptable DoF**: any range with boundaries included within 32-bit integer limits.
- **Usage**: suitable for usage with and without replacement.
- **Security**: not suitable for cryptographic secure purposes.
- **OS/System version and constraints**: none - implementation is OS/System independent and uses only low-level operators.

APPENDIX B: Result of testing

```
#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|       rngcert_1497880246504.dat|  3.42e+07  |
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
   diehard_birthdays|   0|       100|     100|0.25687286|  PASSED
      diehard_operm5|   0|   1000000|     100|0.52281045|  PASSED
  diehard_rank_32x32|   0|     40000|     100|0.91402132|  PASSED
    diehard_rank_6x8|   0|    100000|     100|0.70005033|  PASSED
   diehard_bitstream|   0|   2097152|     100|0.53827306|  PASSED
        diehard_opso|   0|   2097152|     100|0.74608804|  PASSED
        diehard_oqso|   0|   2097152|     100|0.78833077|  PASSED
         diehard_dna|   0|   2097152|     100|0.35716668|  PASSED
diehard_count_1s_str|   0|    256000|     100|0.33540860|  PASSED
diehard_count_1s_byt|   0|    256000|     100|0.88109230|  PASSED
 diehard_parking_lot|   0|     12000|     100|0.69799899|  PASSED
    diehard_2dsphere|   2|      8000|     100|0.47012826|  PASSED
    diehard_3dsphere|   3|      4000|     100|0.04895489|  PASSED
     diehard_squeeze|   0|    100000|     100|0.78648999|  PASSED
        diehard_sums|   0|       100|     100|0.02830501|  PASSED
        diehard_runs|   0|    100000|     100|0.43851988|  PASSED
        diehard_runs|   0|    100000|     100|0.14895430|  PASSED
       diehard_craps|   0|    200000|     100|0.19602121|  PASSED
       diehard_craps|   0|    200000|     100|0.21639467|  PASSED
# The file file_input_raw was rewound 1 times
 marsaglia_tsang_gcd|   0|  10000000|     100|0.79684392|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.99000600|  PASSED
# The file file_input_raw was rewound 1 times
         sts_monobit|   1|    100000|     100|0.38104907|  PASSED
# The file file_input_raw was rewound 1 times
            sts_runs|   2|    100000|     100|0.03680668|  PASSED
# The file file_input_raw was rewound 1 times
          sts_serial|   1|    100000|     100|0.36977340|  PASSED
          sts_serial|   2|    100000|     100|0.94081086|  PASSED
          sts_serial|   3|    100000|     100|0.53179791|  PASSED
          sts_serial|   3|    100000|     100|0.43593212|  PASSED
          sts_serial|   4|    100000|     100|0.94739130|  PASSED
          sts_serial|   4|    100000|     100|0.14192131|  PASSED
          sts_serial|   5|    100000|     100|0.05259254|  PASSED
          sts_serial|   5|    100000|     100|0.08352908|  PASSED
          sts_serial|   6|    100000|     100|0.71004194|  PASSED
          sts_serial|   6|    100000|     100|0.74110529|  PASSED
          sts_serial|   7|    100000|     100|0.64097142|  PASSED
          sts_serial|   7|    100000|     100|0.43802822|  PASSED
          sts_serial|   8|    100000|     100|0.55125174|  PASSED
          sts_serial|   8|    100000|     100|0.99431885|  PASSED
          sts_serial|   9|    100000|     100|0.54531040|  PASSED
          sts_serial|   9|    100000|     100|0.55848305|  PASSED
```

```
          sts_serial|  10|    100000|     100|0.35842976|  PASSED
          sts_serial|  10|    100000|     100|0.86497293|  PASSED
          sts_serial|  11|    100000|     100|0.55604986|  PASSED
          sts_serial|  11|    100000|     100|0.96062507|  PASSED
          sts_serial|  12|    100000|     100|0.57074637|  PASSED
          sts_serial|  12|    100000|     100|0.63101745|  PASSED
          sts_serial|  13|    100000|     100|0.93771149|  PASSED
          sts_serial|  13|    100000|     100|0.98345249|  PASSED
          sts_serial|  14|    100000|     100|0.75568901|  PASSED
          sts_serial|  14|    100000|     100|0.78082276|  PASSED
          sts_serial|  15|    100000|     100|0.94403009|  PASSED
          sts_serial|  15|    100000|     100|0.69119997|  PASSED
          sts_serial|  16|    100000|     100|0.82531133|  PASSED
          sts_serial|  16|    100000|     100|0.92306020|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   1|    100000|     100|0.27350791|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   2|    100000|     100|0.26046075|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   3|    100000|     100|0.74269671|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   4|    100000|     100|0.74497896|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   5|    100000|     100|0.81607916|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   6|    100000|     100|0.68227251|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   7|    100000|     100|0.61765644|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   8|    100000|     100|0.08060607|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|   9|    100000|     100|0.72326853|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|  10|    100000|     100|0.18962473|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|  11|    100000|     100|0.92295973|  PASSED
# The file file_input_raw was rewound 1 times
         rgb_bitdist|  12|    100000|     100|0.57704902|  PASSED
# The file file_input_raw was rewound 1 times
rgb_minimum_distance|   2|     10000|    1000|0.35424346|  PASSED
# The file file_input_raw was rewound 1 times
rgb_minimum_distance|   3|     10000|    1000|0.69424283|  PASSED
# The file file_input_raw was rewound 1 times
rgb_minimum_distance|   4|     10000|    1000|0.62818046|  PASSED
# The file file_input_raw was rewound 1 times
rgb_minimum_distance|   5|     10000|    1000|0.05641253|  PASSED
# The file file_input_raw was rewound 1 times
    rgb_permutations|   2|    100000|     100|0.86128952|  PASSED
# The file file_input_raw was rewound 1 times
    rgb_permutations|   3|    100000|     100|0.20369892|  PASSED
# The file file_input_raw was rewound 1 times
```

```
    rgb_permutations|   4|    100000|     100|0.90382777|  PASSED
# The file file_input_raw was rewound 1 times
    rgb_permutations|   5|    100000|     100|0.15907545|  PASSED
# The file file_input_raw was rewound 1 times
      rgb_lagged_sum|   0|   1000000|     100|0.43795261|  PASSED
# The file file_input_raw was rewound 1 times
      rgb_lagged_sum|   1|   1000000|     100|0.75212288|  PASSED
# The file file_input_raw was rewound 1 times
      rgb_lagged_sum|   2|   1000000|     100|0.68892430|  PASSED
# The file file_input_raw was rewound 2 times
      rgb_lagged_sum|   3|   1000000|     100|0.98642391|  PASSED
# The file file_input_raw was rewound 2 times
      rgb_lagged_sum|   4|   1000000|     100|0.36042162|  PASSED
# The file file_input_raw was rewound 2 times
      rgb_lagged_sum|   5|   1000000|     100|0.73451797|  PASSED
# The file file_input_raw was rewound 2 times
      rgb_lagged_sum|   6|   1000000|     100|0.97722946|  PASSED
# The file file_input_raw was rewound 2 times
      rgb_lagged_sum|   7|   1000000|     100|0.97447032|  PASSED
# The file file_input_raw was rewound 3 times
      rgb_lagged_sum|   8|   1000000|     100|0.34834258|  PASSED
# The file file_input_raw was rewound 3 times
      rgb_lagged_sum|   9|   1000000|     100|0.48882961|  PASSED
# The file file_input_raw was rewound 3 times
      rgb_lagged_sum|  10|   1000000|     100|0.46908464|  PASSED
# The file file_input_raw was rewound 4 times
      rgb_lagged_sum|  11|   1000000|     100|0.93297545|  PASSED
# The file file_input_raw was rewound 4 times
      rgb_lagged_sum|  12|   1000000|     100|0.52446016|  PASSED
# The file file_input_raw was rewound 5 times
      rgb_lagged_sum|  13|   1000000|     100|0.56248723|  PASSED
# The file file_input_raw was rewound 5 times
      rgb_lagged_sum|  14|   1000000|     100|0.53069740|  PASSED
# The file file_input_raw was rewound 6 times
      rgb_lagged_sum|  15|   1000000|     100|0.98392826|  PASSED
# The file file_input_raw was rewound 6 times
      rgb_lagged_sum|  16|   1000000|     100|0.19640395|  PASSED
# The file file_input_raw was rewound 7 times
      rgb_lagged_sum|  17|   1000000|     100|0.92160780|  PASSED
# The file file_input_raw was rewound 8 times
      rgb_lagged_sum|  18|   1000000|     100|0.02169035|  PASSED
# The file file_input_raw was rewound 8 times
      rgb_lagged_sum|  19|   1000000|     100|0.98564005|  PASSED
# The file file_input_raw was rewound 9 times
      rgb_lagged_sum|  20|   1000000|     100|0.13578079|  PASSED
# The file file_input_raw was rewound 10 times
      rgb_lagged_sum|  21|   1000000|     100|0.21476112|  PASSED
# The file file_input_raw was rewound 10 times
      rgb_lagged_sum|  22|   1000000|     100|0.56530150|  PASSED
# The file file_input_raw was rewound 11 times
      rgb_lagged_sum|  23|   1000000|     100|0.62395215|  PASSED
```

```
      rgb_lagged_sum|  24|   1000000|     100|0.57184532|  PASSED
# The file file_input_raw was rewound 13 times
      rgb_lagged_sum|  25|   1000000|     100|0.17433345|  PASSED
# The file file_input_raw was rewound 14 times
      rgb_lagged_sum|  26|   1000000|     100|0.98649945|  PASSED
# The file file_input_raw was rewound 15 times
      rgb_lagged_sum|  27|   1000000|     100|0.64529337|  PASSED
# The file file_input_raw was rewound 16 times
      rgb_lagged_sum|  28|   1000000|     100|0.98961403|  PASSED
# The file file_input_raw was rewound 17 times
      rgb_lagged_sum|  29|   1000000|     100|0.38588344|  PASSED
# The file file_input_raw was rewound 18 times
      rgb_lagged_sum|  30|   1000000|     100|0.24135769|  PASSED
# The file file_input_raw was rewound 19 times
      rgb_lagged_sum|  31|   1000000|     100|0.98886878|  PASSED
# The file file_input_raw was rewound 20 times
      rgb_lagged_sum|  32|   1000000|     100|0.98516932|  PASSED
# The file file_input_raw was rewound 20 times
     rgb_kstest_test|   0|     10000|    1000|0.50747795|  PASSED
# The file file_input_raw was rewound 20 times
     dab_bytedistrib|   0|  51200000|       1|0.85358037|  PASSED
# The file file_input_raw was rewound 20 times
           dab_dct| 256|     50000|       1|0.51736758|  PASSED
Preparing to run test 207.  ntuple = 0
# The file file_input_raw was rewound 20 times
        dab_filltree|  32|  15000000|       1|0.28344744|  PASSED
        dab_filltree|  32|  15000000|       1|0.50403136|  PASSED
Preparing to run test 208.  ntuple = 0
# The file file_input_raw was rewound 20 times
       dab_filltree2|   0|   5000000|       1|0.26877043|  PASSED
       dab_filltree2|   1|   5000000|       1|0.03735815|  PASSED
Preparing to run test 209.  ntuple = 0
# The file file_input_raw was rewound 20 times
        dab_monobit2|  12|  65000000|       1|0.16805524|  PASSED
```

APPENDIX C: Software digital signature

File name	SHA1
\sw-random\src\index.ts	d5aab80fbbb91dc610baf439fd8e5eaa3d9d1f8c
\sw-random\src\skywind\random.ts	68cbd1bd1ee7d4e0725a23d79d8a2a0888c274e0
mersenne-twister.js	87b1ea3b7d5b16feb1c9e4b836f65d5a9b2eaf14