QUANTIS CERTIFICATIONS

April 2016

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge / Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com
www.idquantique.com

Introduction

Random number generation needs to be unfailingly reliable. Poor quality randomness (often also called entropy") means that the output bit stream may be predictable and therefore easily guessed or emulated. This predictability means poor security for the application using the random bits.

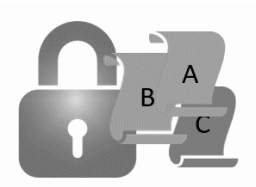
Pseudo random number generators based on software are not capable of providing true randomness as they are based on deterministic computer programs. Instead they rely on external entropy sources to build up randomness. **This can be a major vulnerability for pseudo RNGs in data centers or networks where there is not enough external entropy to seed the RNGs.**

Quantis: the most trusted and certified RNG in the market

For some companies, the quality of their RNG's "random" output is nothing more than a check box. They want to feel that they have covered their compliance requirements, and that check box is the finish line as far as they are concerned. For ID Quantique, randomness quality is at the very core of the Quantis offering.

This is why we want to reach **more than just compliance with the NIST test suite**.

We strive to successfully pass every set of tests, be it NIST or DIE HARD, and to reach the most demanding standards like the German BSI's AIS 31. We also use reputed accredited test institutions such as the English CTL, the French ANSSI or the Swiss METAS to ensure national independence and quality. IDQ follows best practices and continually performs quality and security testing. Because we know that quality and security standards are not a one time achievement, and since the hackers technology keeps improving, so should our level of security.



Moreover, **no single certification should be considered a sufficient assurance of quality**. Some compliance testing laboratories may have national affiliations which may impact the independence of the testing. This is why being certified by **different national institutions, independent** of each other, is the proper way to ensure the quality of your RNG.

With this underlying philosophy, ID Quantique has successively submitted new generations of the Quantis family to several laboratories over the years since the first release in 2001. Below you will find a list of the different tests which Quantis has successfully passed.

A. NIST : SP800-22 Test Suite Compliance

The National Institute for Standards and Technology (NIST) is the US agency dedicated to setting new standards in every technological field: bioscience / energy / communication / etc. Regarding IT security, the NIST standards are designed for the American federal agency security level, which makes them highly trustworthy.

The Quantis has been submitted to the NIST Special Publication 800-22 named "**A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications**" and successfully passed all the test suites.

The SP800-22 is a collection of statistical tests which evaluates the randomness extracted from a generator. It includes:

1. The frequency (monobits) test
2. The frequency test within a block
3. The runs test
4. The test for the longest run of ones in a block
5. The binary matrix rank test
6. The discrete Fourier transform (spectral) test
7. The non-overlapping template matching test
8. The overlapping template matching test
9. The Maurer's "universal statistical" test
10. The linear complexity test
11. The serial test
12. The approximate entropy test
13. The cumulative sums (Cusum) test
14. The random excursions test
15. The random excursions variant test

For each of these tests the Quantis was recognized as random.

The Quantis compliance to the SP800-22 test suite was conducted internally at ID Quantique. Indeed the NIST does not perform itself any evaluation leading to an official certification, it only offers its statistical tests to individuals or enterprises who want to check their own products.

NIST SP800-22: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

B. METAS Certification

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Swiss Federal Bureau of Metrology (METAS), is part of the Swiss Federal Department of Justice and Police. It is the Swiss national reference in compliance testing.

The randomness of the Quantis was evaluated by METAS using the **DIEHARD battery of tests**. This test suite includes:

1. The birthday spacings test
2. The overlapping 5-permutations test
3. The ranks of matrices test
4. The ranks of bits test
5. The missing word test
6. The overlapping pairs sparse occupancy test
7. The counts the 1s test for successive bytes
8. The counts the 1s test for specific bytes
9. The parking lot test
10. The minimum distance test
11. The random spheres test
12. The squeeze test
13. The overlapping sums test
14. The runs test
15. The craps test

For each of these tests the Quantis was recognized as random.

The METAS certification for the Quantis USB / PCI / PCIe was issued the 10th May 2010 by the Berne-Wabern METAS laboratory.

Quantis METAS certification: http://marketing.idquantique.com/acton/attachment/11868/f-0043/1/-/-/-/-/Metas%20Certificate.pdf

C. CTL Certification

The Compliance Testing Laboratory (CTL), located in Bangor, UK, is the English organization which undertakes testing of both gaming software and gaming machines in accordance with the UK Gambling Commission's standards.

The CTL is accredited to ISO/IEC 17025:2005 for the UKGC technical standards and performs auditing and consultancy for ISP/IEC 27001:2005 for Information Security Management Systems.

The randomness of the Quantis was evaluated by the CTL on 2011 and the device passed their randomness tests successfully.

The CTL certification for the Quantis USB / PCI / PCIe was issued the 30th March 2011 by the Bangor CTL laboratory, UK.

Quantis CTL certification: http://www.idquantique.com/wordpress/wpcontent/uploads/CTLCompliance-Certificate

D. iTech Labs Certificate

Several installations of Quantis used for gaming applications have been, on customer's request, tested and certified by iTech Labs.

Based in Melbourne, Australia, iTech Labs' Hardware Random Number Generators using the DIEHARD battery of tests. The DIEHARD tests include the following:

1. Birthday spacings
2. Overlapping 5-permutations
3. Binary rank test for 31x31 matrices
4. Binary rank test for 32x32 matrices
5. Binary rank test for 6x8 matrices
6. Bit-stream tests on 20-bit words
7. Bit-stream tests OPSO, OQSO, DNA
8. Count-the-1's in a stream of bytes
9. Count-the-1's in specific bytes
10. Parking lot test
11. Minimum distance test
12. The 3dspheres test
13. The squeeze test
14. Overlapping sums test
15. Runs test
16. Craps test

iTech Labs is an ISO/IEC 17025 certified testing laboratory for online gaming systems.

iTech Labs – RNG Testing & Certification:
http://www.itechlabs.com.au/sidebar-eng/rng-testing-certification/

E. BSI AIS 31 Compliance (dedicated version of Quantis)

The AIS 31 evaluation methodology is a test suite developed by the German Federal Office for Information Security (BSI) - the German federal agency in charge of managing computer and communication security for the government. This is one of the most stringent test suites on the market.

The AIS 31 compliance test, if successfully passed, ranks an RNG on a 3 levels scale: PTG.1, PTG.2 and PTG.3. The QUANTIS AIS31 achieved PTG.3 level, which allows it to be used in strongly regulated gaming or security markets.

RNG Class	Comment
PTG.1	Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers
PTG.2	PTG.1, additionally a stochastic model of the entropy source and statistical tests of the raw random numbers
PTG.3	PTG.2, additionally with cryptographic post-processing (hybrid PTRNG)

QUANTIS compliance to the AIS 31 standard has been tested by the CESTI-LETI (CEA Grenoble) and validated by the French National Agency for Security of Information Systems (ANSSI) according to the AIS 31 methodology defined by the German Federal Office for Information Security (BSI).

The validation of the AIS 31 PTG.3 level was issued by the ANSSI the 19th August 2014. It applies only to dedicated AIS31 versions of Quantis (QUANTIS AIS31) which are provided with the certified post-processing software.

Quantis AIS31-dedicated version, AIS31 compliance certificate:
http://marketing.idquantique.com/acton/attachment/11868/f-0040/1/-/-/-/-/AIS31%20Test%20Report.pdf

AIS31 methodology by the BSI:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile