PRESS RELEASE

30 SEPTEMBER 2014 | GENEVA, SWITZERLAND

ID Quantique launches world's most rigorously tested quantum random number generators

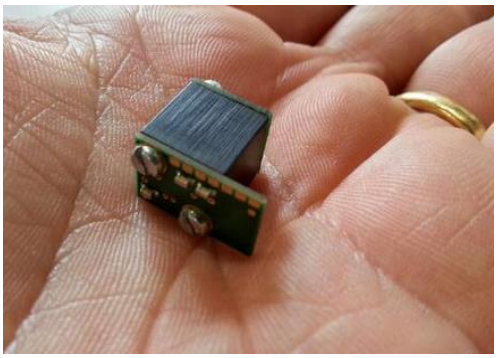
THE QUANTUM DEVICES CLEAR AIS 31 TESTING, WIDENING THE OPTIONS FOR HEAVILY REGULATED MARKETS

ID Quantique SA (IDQ) today announced the launch of the Quantis AIS 31 family of Random Number Generators. The Quantis AIS31 range have met the rigors of AIS 31 testing, expanding their customer base to new, strongly regulated markets.

"Our team is dedicated to bringing quantum-based security products to the commercial market at large," says Gregoire Ribordy, co-founder and CEO of ID Quantique, "Quantis is the first quantum random number generator to reach this level of compliance; eliminating the risk of software-based RNGs and offering regulated industries true randomness. When the generation of random numbers cannot be left to chance, Quantis is the solution."

Random number generation (RNG) is a critical requirement for security and reliability in many demanding applications. Unlike software, which relies on a finite number of options, quantum physics is inherently random and therefore an excellent source of randomness.

IDQ's Quantis RNG is a compact, low cost and easy-to-use random number generator exploiting a quantum optical process as a source of truly unpredictable randomness. The process takes place in the cube (pictured right) which is, in effect, the world's first quantum coprocessor. It features a high bit-rate output stream, which does not exhibit any correlations, passes all statistical tests and is robust to environmental influences.



Now, having passed the globally recognized testing standards of AIS 31, the Quantis products can be leveraged in more heavily regulated markets such as finance and gaming. The BSI-based AIS 31 methodology validates several aspects of a hardware random number generator; including the device's capability to detect failures of the entropy (randomness) source and the presence of non-tolerable statistical defects of the internal random numbers.

The device also benefits from the availability of a stochastic model to represent the probability distribution of the entropy source and statistical tests of the raw random numbers. Quantis comes with a dedicated software library that processes the output of the generator according to the AIS 31 specifications.

In terms of performance, the Quantis AIS 31 provides additional cryptographic post-processing that enhances the quality of the random output with forward and backward secrecy. This means that previous or future numbers cannot be predicted, even if the internal state of the random number generator is known. This is essential in preventing hacking.

In addition to the high quality of the random numbers being produced, the devices are also subjected to more intensive environmental testing, which brings assurance that they will perform in even harsher environments beyond the office.

Quantis AIS 31 is a Swiss Quantum product that benefits from having been designed and built in Switzerland, adding the globally recognized guarantee of quality and independence.

SWISS QUANTUM

About ID Quantique SA

IDQ
REDEFINING CERTAINTY

ID Quantique is a leader in long-term data security; offering high-performance, multi-protocol network encryption based on conventional and quantum technologies. The company provides network security products and services to banks, governments and other enterprises globally.

IDQ also has a global footprint for quantum-based scientific instrumentation products (measuring devices for academic and industrial research laboratories) and random number generators. The company was founded in 2001 and is based in Geneva, Switzerland. www.idquantique.com