

# USER CASE

### REDEFINING RANDOMNESS

## Loterie Romande



### Quantum Draws for Lottery Games in Switzerland

Quantis True Random Number Generator in Lottery Application

"Beyond the technical specifications of the Quantis random number generators, we were very impressed by the support offered by IDQ. Whenever a question arises, it is very easy to get hold of a specialist and our requests are always handled very promptly"

Bertrand Ménard, Game Specialist at Loterie Romande

#### **Quantis-PCIe-4M**



Quantis is a familly of true random number generators (TRNG), based on quantum physics. Their main features include:

- Certified by Swiss National Laboratory
- Bit rate: 4 or 16 Mbps
- Low cost
- Compact and reliable
- Continuous status check

Copyright© 2011 ID Quantique SA - All rights reserved Loterie Romande User Case v1.0 - October 2011

### The Challenge

The Loterie Romande (www.loro.ch) is one of the two lottery operators in Switzerland. Its activities are focused on French speaking Switzerland and it generated revenues of 360 million Swiss Francs (400 million USD) in 2010. It operates several lottery games with daily draws. The player can buy tickets at a point of sales and the winning numbers are drawn once a day and announced publicly. The draw frequency makes it impossible to use mechanical draws, which are too complicated and costly. Because of this, the company introduced an electronic drawing platform. In 2010, this platform had to be modernized and the Lottery decided to replace the pseudo random number generator, which had been used until then, by a true random number generator. The challenge was to find a physical random number generator providing outstanding randomness quality, reliable operation and ease of integration.

### The Solution

After careful evaluation, the Loterie Romande selected IDQ's Quantis random number generator (RNG), which met all its criteria. Quantis is a family of hardware RNG's, which exploits a quantum optics process to produce random bits. Single light particles, also known as photons, are sent onto a semi-transparent mirror where they are randomly reflected or transmitted. A binary value is associated with each outcome. The fundamental laws of quantum physics guarantee that the bit stream produced by Quantis is truly random. The generator produces a random stream of 4 million bits per second, which can be scaled and mapped to produce suitable random numbers for each gaming application.

The Quantis RNG has been evaluated and certified by specialists at the Swiss Federal Office of Metrology (METAS), who confirmed the quality of the randomness produced. The Loterie Romande also commissioned a second independent evaluation by mathematicians, which confirmed the positive results of the first certification.

In this application, a Quantis RNG in the form of a PClexpress expansion card is inserted in a server, which is then sealed. In order to ensure redundancy, the complete solution runs on two servers, each with a Quantis RNG card. The application for drawing the electronic winning number was developed by the French company LotSys.

