Redefining Randomness

Use Case: Gaming Industry

SWISS QUANTUM

Implementing Quantum Draws to Secure Lotteries

Quantis True Random Number Generator

Customer: Loterie Romande

Industry: Lottery

Country: Switzerland

LOTERIE ROMANDE

Business need	Solution	Results
?	✎	🏆
A random number generator that provides outstanding randomness quality, reliable operation and easy integration.	Quantis random number generator (QRNG), PCI express card (PCIe-4M).	A reliable, easy to use source of true randomness, generating 100% trust.

Business need

The Loterie Romande (www.loro.ch) is one of two lottery operators in Switzerland. Its activities are focused on lottery games and sport betting in the six cantons of the French speaking part of Switzerland and it generated revenues of 398 million Swiss Francs (400 million USD) in 2016.

It operates several lottery games with daily draws. The player can buy tickets at a point of sale 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 Loterie Romande wanted to find a physical random number generator providing outstanding randomness quality, reliable operation and ease of integration.

Solution

The Loterie Romande selected ID Quantique's Quantis random number generator (QRNG), 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 semitransparent 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.

In addition the operation of Quantis is continuously monitored and if a failure is detected, the random bit stream is immediately disabled

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 PCI express 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.

Results

Not only does the solution provide true randomness which is absolutely fundamental for the Loterie Romande but they appreciated the fact that it is also easy to manage.

The Quantis interfaces are open and easy to use. Contrary to many "black boxes", this offers the flexibility and the transparency they were looking for. They can access to and update the application in real time without impacting the security of Quantis. It's 100% trust.

The Loterie Romande has been using the solution since 2010, which has been working unfailingly since then. They particularly appreciated ID Quantique's level of the customer service, getting quick, easy and professional responses to their questions.

"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"

Mr. Bertrand Ménard,
Game Specialist at Loterie Romande