REDEFINING SECURITY | QUANTUM-SAFE CRYPTO

KEY FACTORY

Secure quantum key generation platform

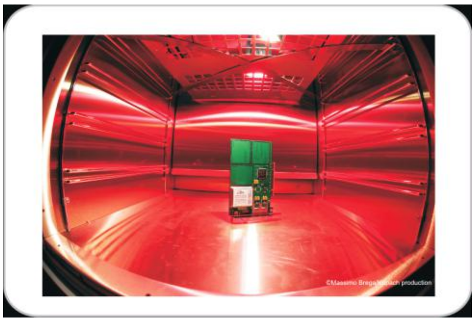
Today's connected world requires constantly higher levels of security. In many situations, this is done by relying on cryptography, for which one of the critical elements is the unpredictability of the encryption keys. Other security applications like identity & access management also require a strong cryptographic foundation based on unique tokens. Digital or paper currencies require unique identifiers that cannot be easily guessed or forecast. In addition, many other high value applications like lotteries, or gaming in general, also require the same capacity to generate totally unpredictable numbers.
The common denominator of all these markets is the critical reliance on absolutely random numbers.

THE SOLUTION

The Quantum Key Factory from ID Quantique (IDQ) is a solution platform for creating cryptographically secure digital keys/tokens, leveraging state of the art technology components. It is based on a modular architecture allowing easy integration into existing projects which require extremely secure digital tokens. These tokens can be cryptographic keys, or any other kind of digital token. (Here the terms “token” and “key” are interchangeable)

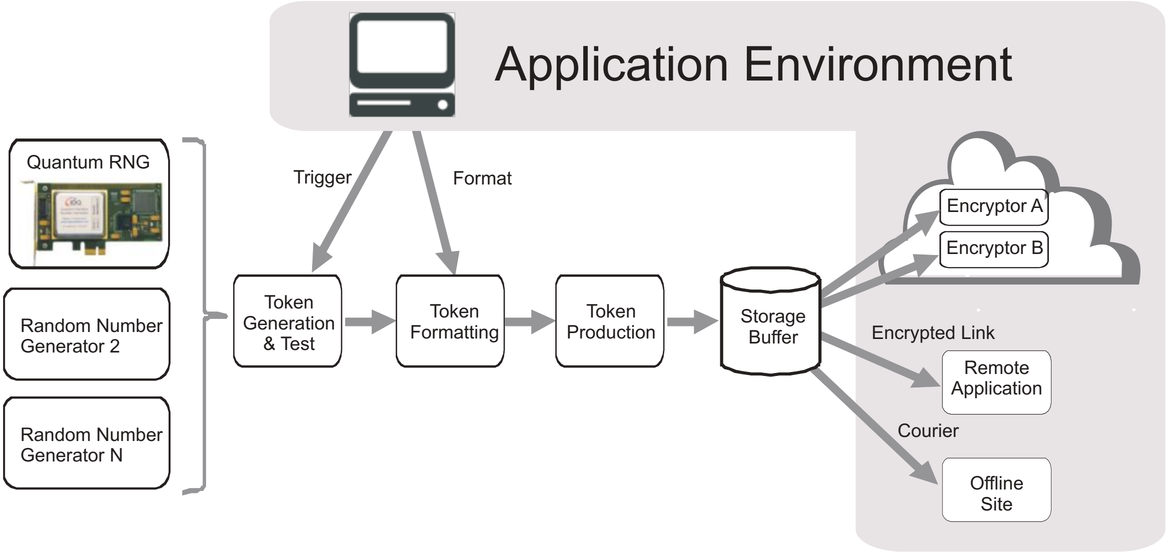
QUANTIS QRNG

The Quantum Key Factory is built on IDQ’s world class, extensively certified Quantis quantum random number generator (QRNG). The Quantum Key Factory is composed of a token generation server which is piloted by a scheduler, and which makes the generated key material available to applications through specific connectors.


©Massimo Brega/Eurelios production

FEATURES

- High quality random number generation for use in most high security applications
- Provably random quantum encryption keys
- Liveness testing for guaranteed performance
- Custom key formats for tailored applications
- Can be integrated into any framework
- Supports multiple entropy sources
- Live testing of randomness (standard algorithms or specific functions)



Key Factory: Modular Architecture

PART 1: TOKEN GENERATION & TESTING

At the heart of the token generation server is a highly sophisticated random number generator which uses potentially several entropy sources to provide the required level of randomness for applications. It can leverage any pre-existing entropy source (either a software Pseudo Random Number Generator, or a hardware True Random Number Generator), and mix it with a bitstream from IDQ’s Quantum Random Number Generator to ensure the best possible entropy, thanks to the provable randomness of the QRNG. An additional advantage is that high quality random numbers are available immediately - even at boot time - since the entropy of the quantum source is always high.

Built-in audit mechanisms control the output of the entropy source. The QRNG comes with its own electronic controls, as well as a stochastic model which enables real-time detection of variations from the normal behavior of the source.

Customised, application-specific auditing mechanisms can also be implemented at this point or later.

The numbers output from the entropy source mixer are then treated by a post-processing module. This can either be a simple pass-through, IDQ's own randomness extractor, an AIS 31 compliant post-processor, or any custom designed post processing that is required by the specific implementation. This provides stream of random numbers of perfectly controlled quality, with all required checks and audit mechanisms in place to ensure the constant quality of the numbers produced.

An auditing module audits the final output, as well as potentially other sources of key material, using standards such as NIST 800-22.

PART 2: TOKEN FORMATTING

From the random numbers produced, a separate module is responsible for triggering the generation of tokens. It is responsible for formatting the tokens per specification of the implementation (key/token size, structure…).

This scheduler is also responsible for triggering the token generation either on a fixed schedule (X tokens per specified period of time), or on request (whenever an application requests a token).

PART 3: TOKEN PRODUCTION

Once keys or tokens are produced, they may be used by the specified application environment.

The next step is to distribute the keys to their place of use. They can be inserted into key management frameworks, such as EKM or PKI using via standard formats (eg. KMIP, X.509).

They can be stored on a secure medium, such as an encrypted USB key, CD, or any other physical medium and distributed manually.

They can also be exchanged over an existing encrypted connection.

If an ultimate trust is required, the produced key material should be exchanged in a quantum-safe manner,for example through use of a Quantum Key Distribution (QKD) solution such as IDQ's Cerberis product line.

APPLICATIONS

A typical application of IDQ’s Quantum Key Factory is the generation of ultra-secure symmetric encryption keys for high sensitivity environments such as military, defense, or high value corporate networks. Other applications include the generation of cryptographically secure tokens for Identity and Access Management, or unique serial numbers, such as those used by national money issuers or digital currencies.

DETAILED SPECIFICATIONS

- **Architecture:**
  - Modular & customisable
- **Hardware Requirements**
  - Quantis-PCIe-16M (x2)
  - Other RNG sources possible
- **Random Number Generation**
  - Number of TRNG's: N
  - Base TRNG's: Quantis-PCIe-16M (2 units)
  - Other RNG's: Any generator with USB or PCI-express interface, any software RNG
  - Key material generation rate: Defined by selected combination of RNGs & by type of Live Test Suite
- **Key Output**
  - Key generation rate: Defined by selected combination of RNGs
- **Bit Stream Mixing**
  - XOR by default
  - Customisable
- **Live Testing**
  - AIS31 Live Test Suite
  - Other tests suites implemented defined by target application

  Remote Key Distribution
- - Key Management Interoperability Protocol (KMIP)
  - Quantum Key Distribution
  - Other options defined by target application
- **Physical Media**
  - Hard disk
  - USB stick
  - Optical disks
  - Other media defined by target application
- **Access Control**
  - Role-based with three roles (Operator, Administrator, Auditor)
- **Advanced Functionalities**:
  - Possibility to test key material from other external sources

Disclaimer
The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.