IDQ

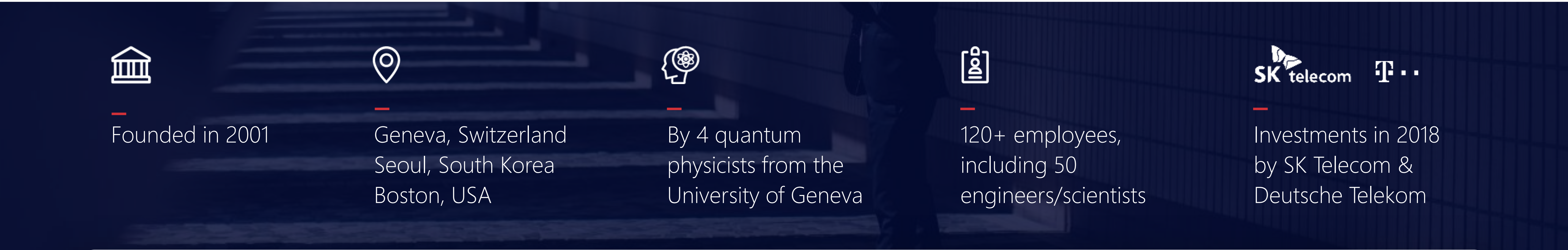
20 YEARS QUANTUM INNOVATION

# ECW
# ID Quantique QRNG

Kevin LAYAT

18/11/2024

# ID Quantique



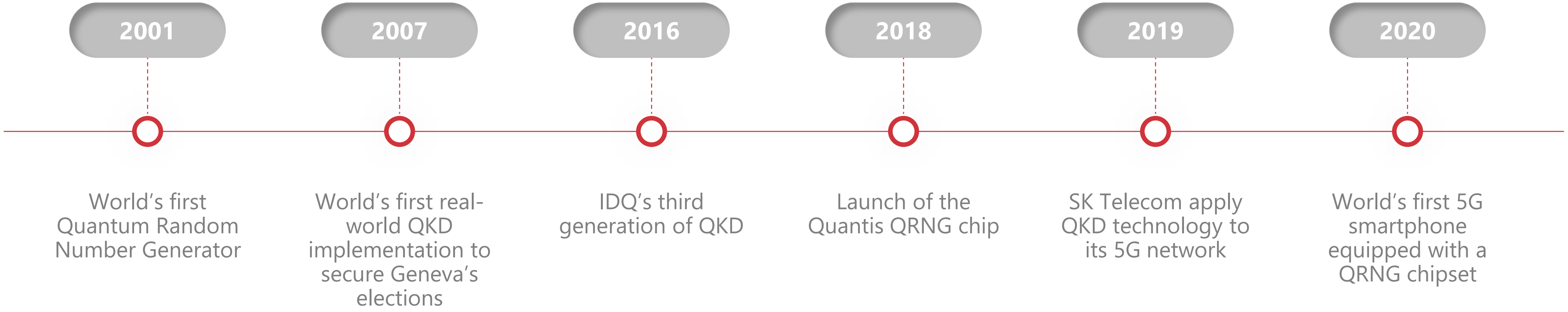
Founded in 2001

Geneva, Switzerland
Seoul, South Korea
Boston, USA

By 4 quantum physicists from the University of Geneva

120+ employees, including 50 engineers/scientists

Investments in 2018 by SK Telecom & Deutsche Telekom



2001 – World's first Quantum Random Number Generator

2007 – World's first real-world QKD implementation to secure Geneva's elections

2016 – IDQ's third generation of QKD

2018 – Launch of the Quantis QRNG chip

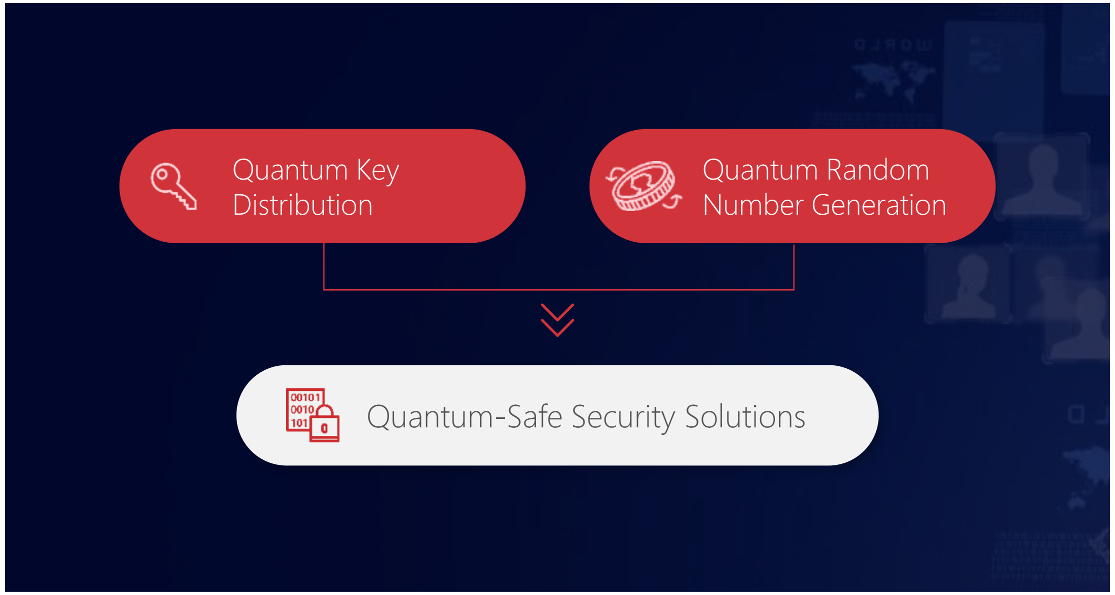
2019 – SK Telecom apply QKD technology to its 5G network

2020 – World's first 5G smartphone equipped with a QRNG chipset

# ID Quantique - divisions & activities

## Quantum-Safe Security

Protecting mission-critical data
*for the long-term future.*



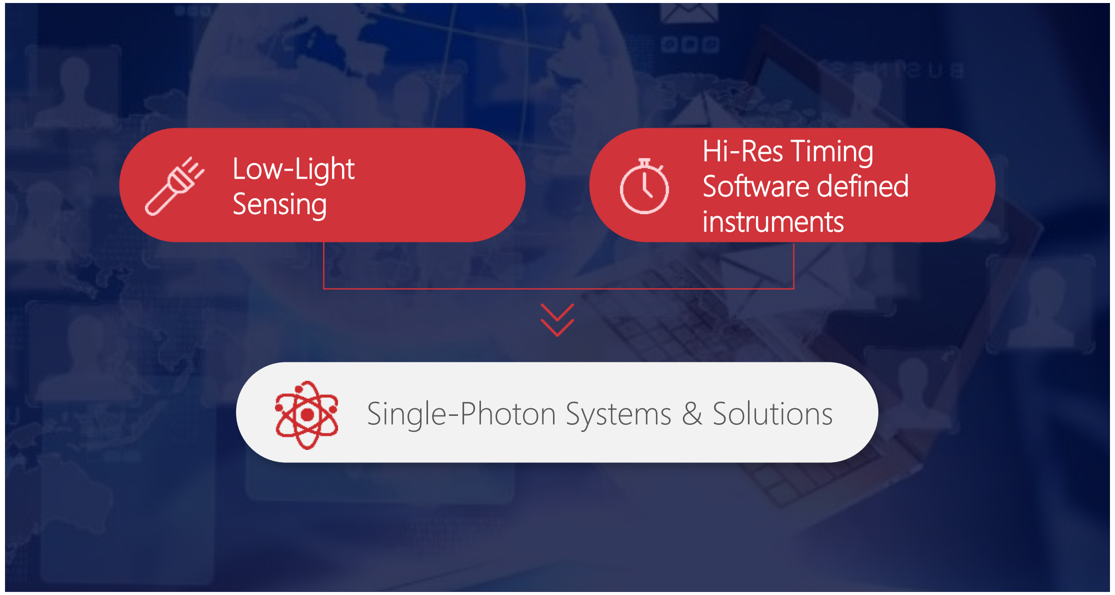
Quantum Key Distribution

Quantum Random Number Generation

Quantum-Safe Security Solutions

## Quantum Sensing

Optical sensing performance beyond conventional techniques,
*creating the building blocks of the Quantum Internet.*



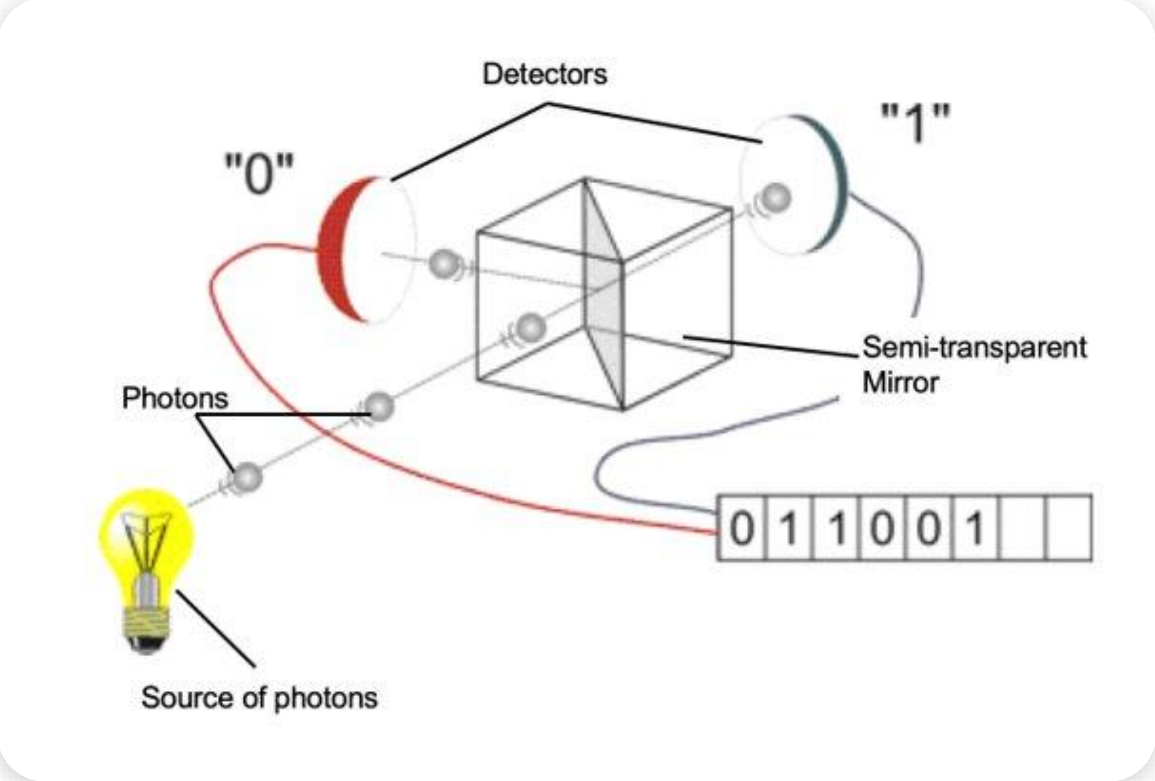
Low-Light Sensing

Hi-Res Timing Software defined instruments

Single-Photon Systems & Solutions

# IDQ’s first ideas

Quantum physics in its simplest form :
a single photon on a beam splitter!



The origin of the random behavior is clear: quantum physics.

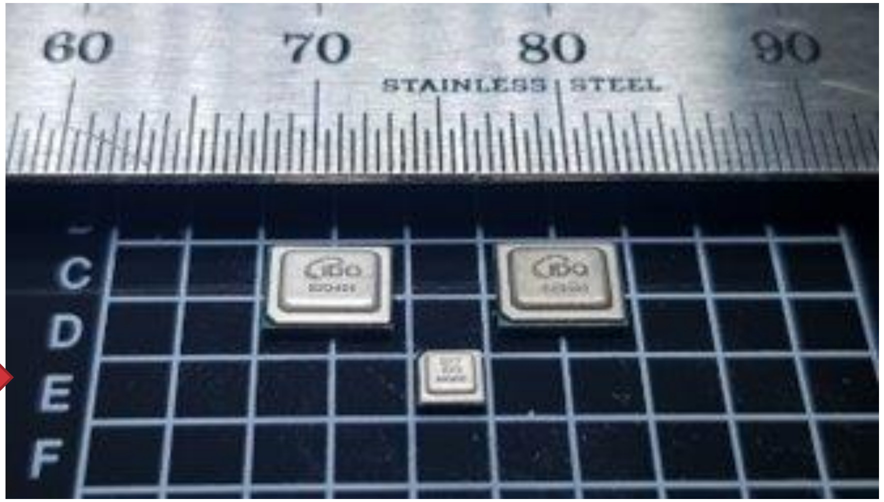
No influence from the environment in the photonic part

Each part can be monitored in real time

# From optical components to chips

Quantis module 44 x 51 mm

SPADs to CMOS Image sensors



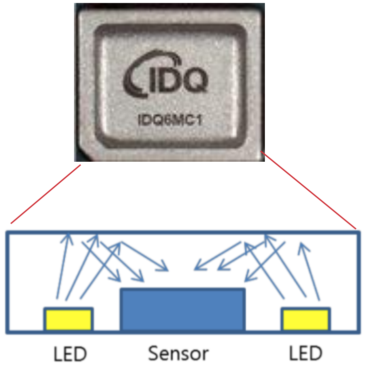
3 QRNG chips

- IDQ6MC1 (6 Mbps entropy, 1.5 Mbps RBG)
- IDQ20MC1 (20 Mbps entropy, 5 Mbps RBG)
- Low-power model (entropy only)

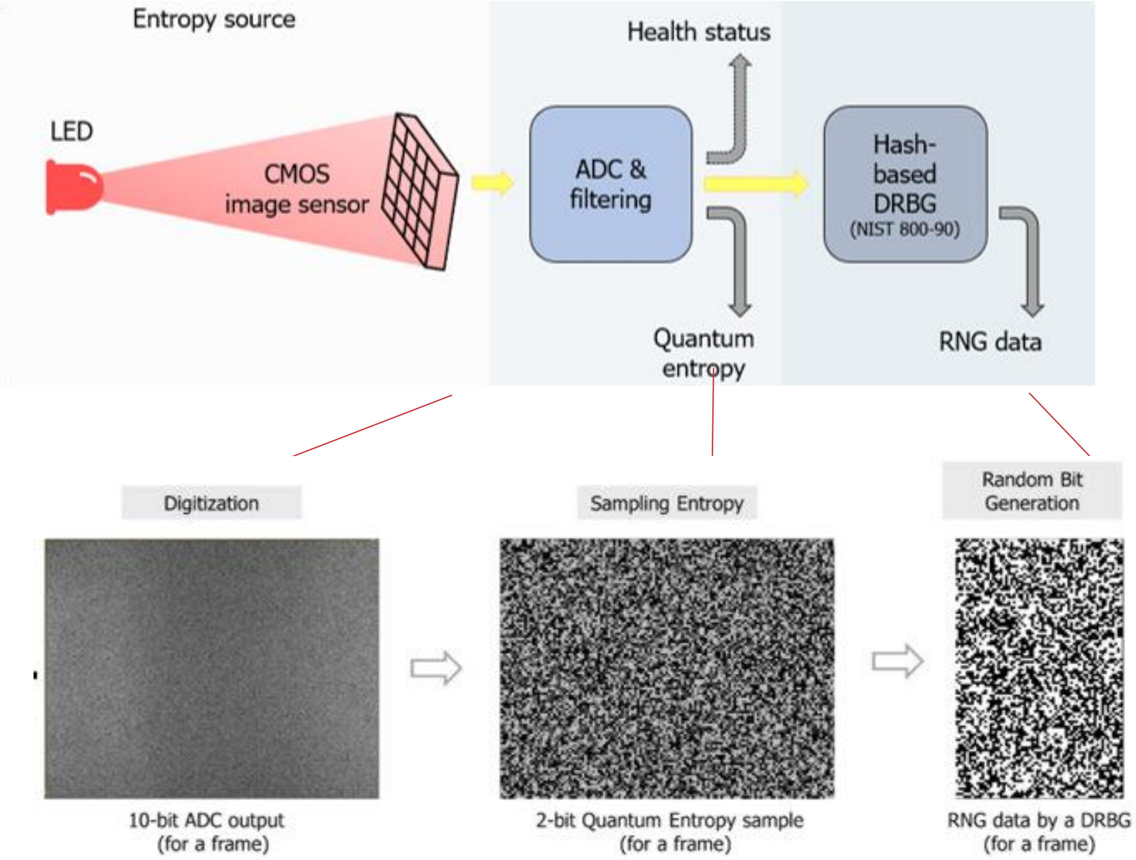
Features

- ≤ 4.2 x 5 mm cross-section
- Low-voltage
- -40°C to +125°C range

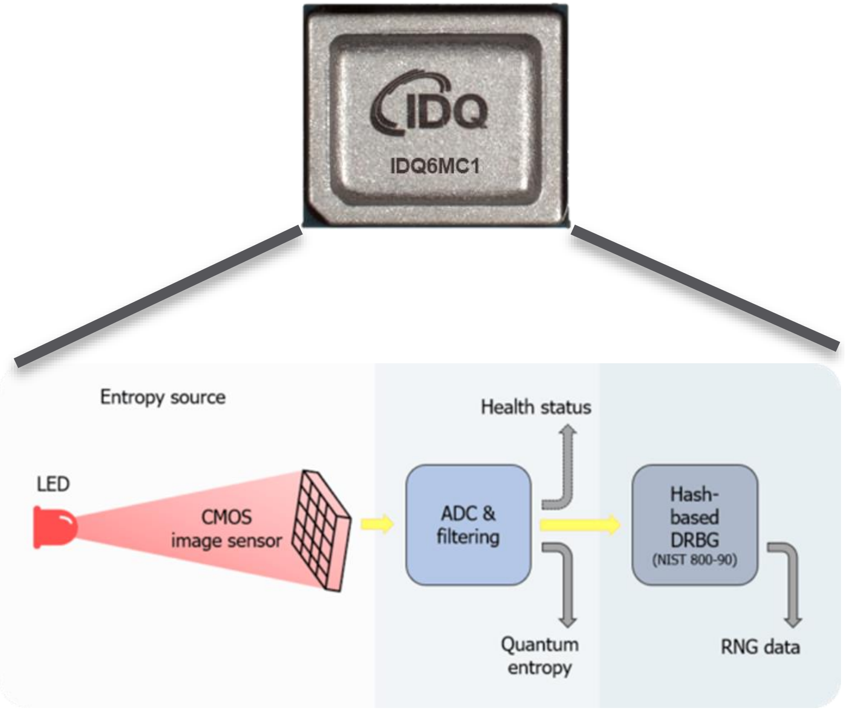
# IDQ's QRNG chips principle



Not perfectly uniform illumination



# Physical model



MSB LSB

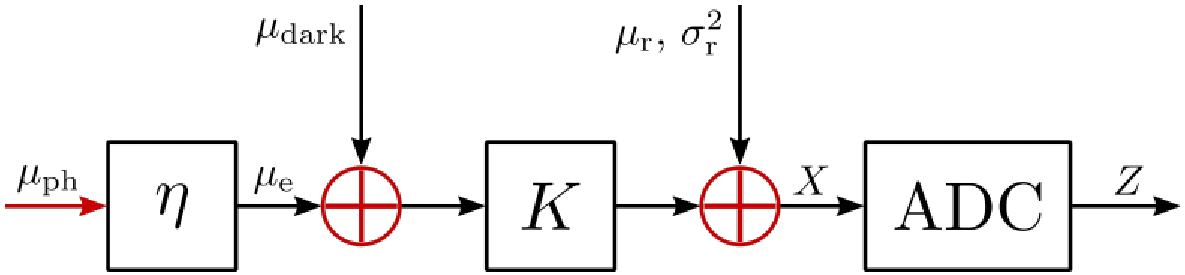
| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

- The number of photon emitted by the LED follows a Poisson distribution :

$$p(n) = \frac{\mu_{ph}^{n} e^{-\mu_{ph}}}{n!}$$

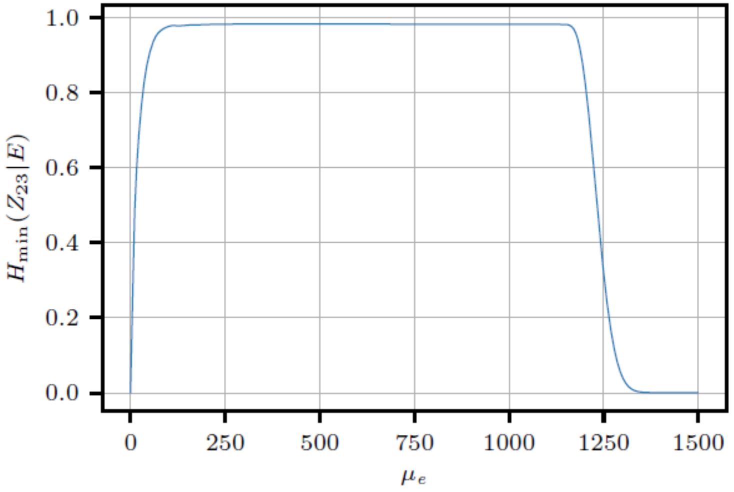
- Each pixel convert the photon into electrons with an efficiency $\eta$. The number of electron also follows a Poisson distribution with parameter $\mu_e$.
- Electrons are converted into a voltage which is then digitized with a 10-bit ADC.
- LSB 2 and 3 are used as quantum entropy.

# Stochatical model



Classical noise E has two contributions :

- One discrete following a Poisson distribution
- One continuous following a normal distribution



# Post-processing

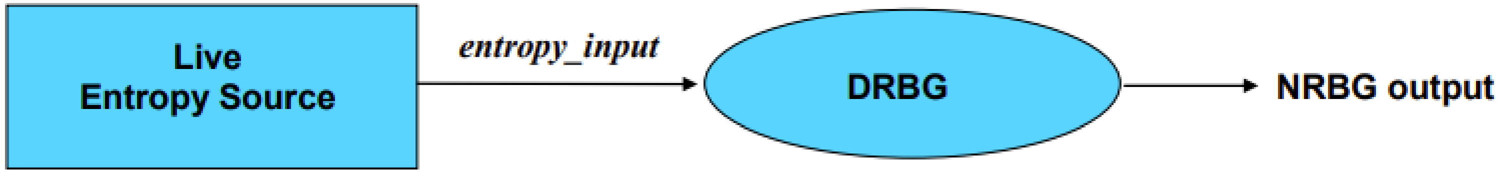


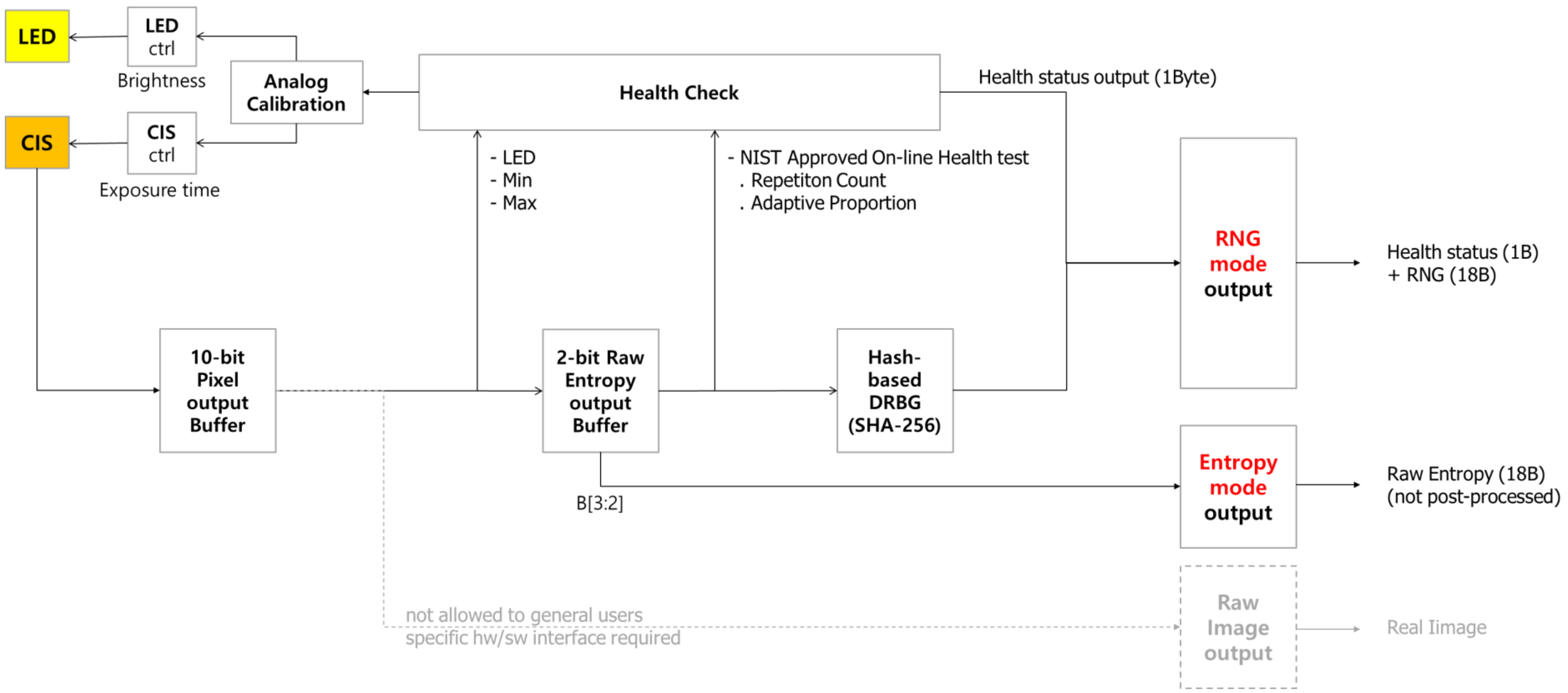
**Figure 7: Enhanced NRBG - Oversampling Construction**

NIST SP800-90 Enhanced NDRBG – Oversampling Construction

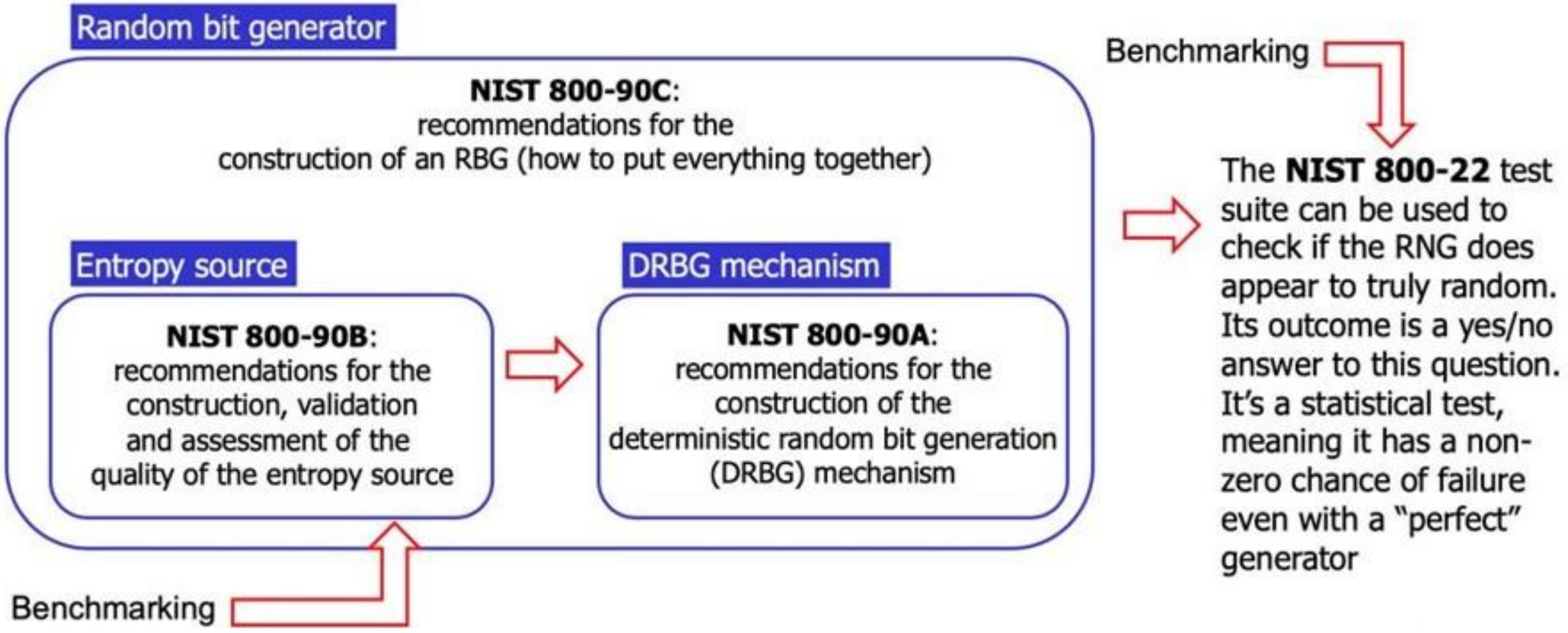
For the Oversampling Construction:

- A Live Entropy Source shall be used, and
- A DRBG mechanism with a prediction resistance capability shall be used that results in one or more reseeds of the DRBG for each request for bits from the NRBG.

# Block diagram



# NIST standard



Random bit generator

**NIST 800-90C**: recommendations for the construction of an RBG (how to put everything together)

Entropy source

**NIST 800-90B**: recommendations for the construction, validation and assessment of the quality of the entropy source

DRBG mechanism

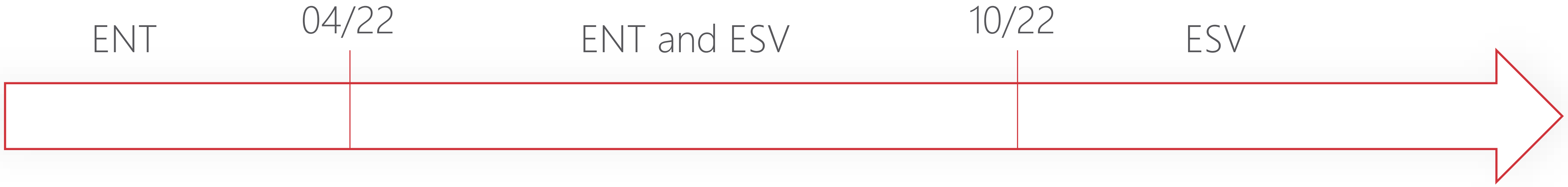
**NIST 800-90A**: recommendations for the construction of the deterministic random bit generation (DRBG) mechanism

Benchmarking

Benchmarking

The **NIST 800-22** test suite can be used to check if the RNG does appear to truly random. Its outcome is a yes/no answer to this question. It's a statistical test, meaning it has a non-zero chance of failure even with a "perfect" generator

# Entropy Validation

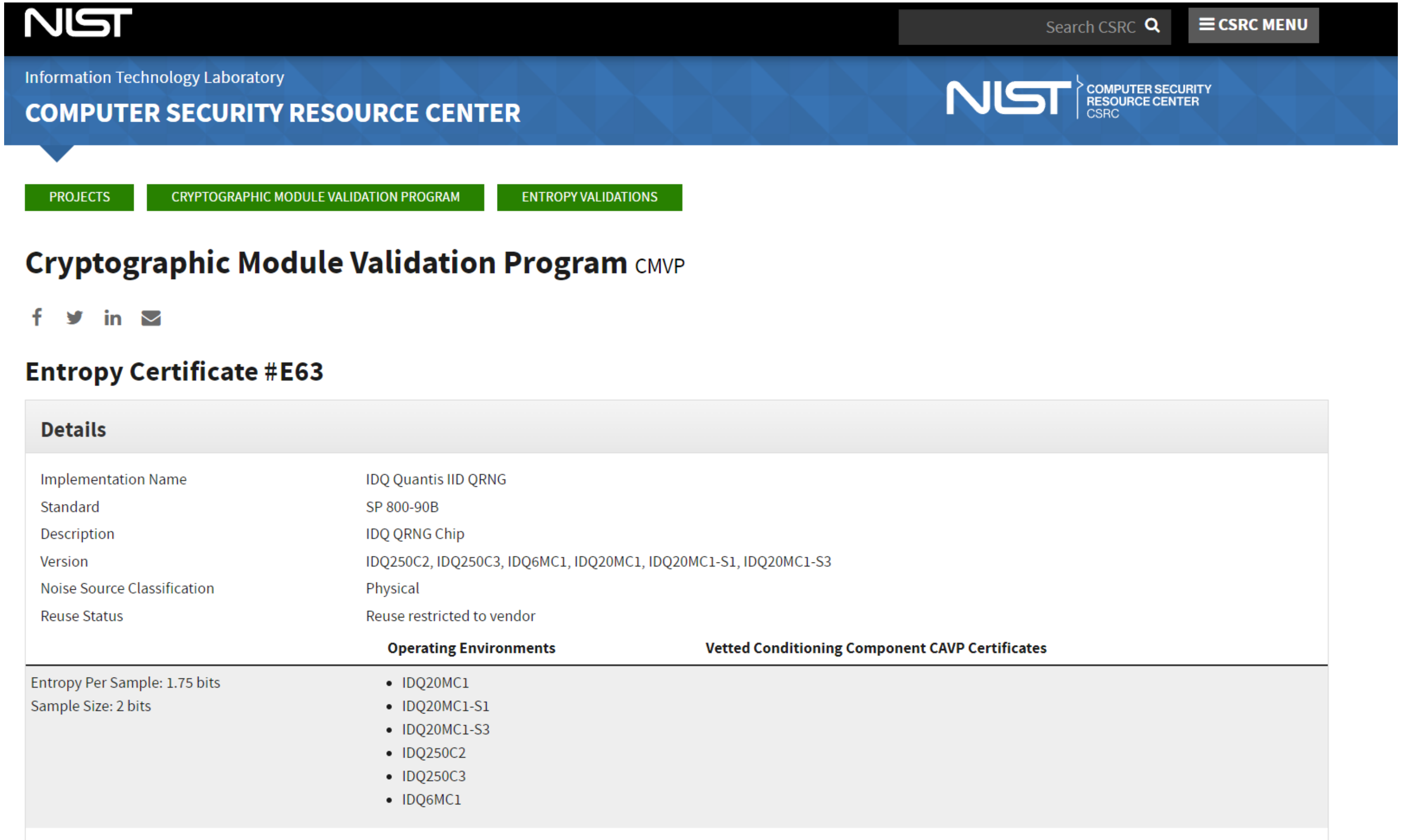


- ENT: former NIST way to validate entropy source
- ESV: Entropy Source Validation; new way to validate an entropy source

- ESV is a standalone certification that means ESV certificates can be ported “as is” to other FIPS modules.

- ESV has 2 tracks : IID and non IID → IDQ is according to NIST IID

# Entropy Validation


NIST
Search CSRC
☰ CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PROJECTS
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM
ENTROPY VALIDATIONS

## Cryptographic Module Validation Program CMVP

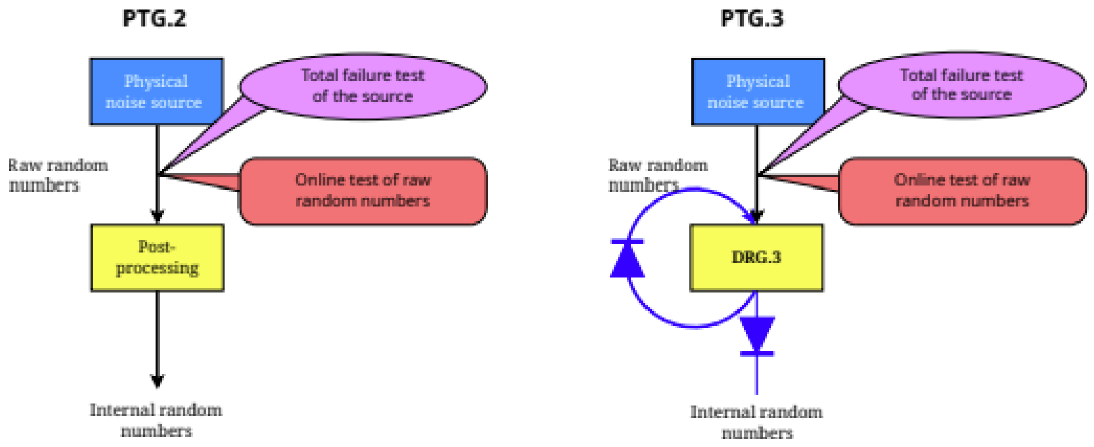
### Entropy Certificate #E63

#### Details

| | |
|---|---|
| Implementation Name | IDQ Quantis IID QRNG |
| Standard | SP 800-90B |
| Description | IDQ QRNG Chip |
| Version | IDQ250C2, IDQ250C3, IDQ6MC1, IDQ20MC1, IDQ20MC1-S1, IDQ20MC1-S3 |
| Noise Source Classification | Physical |
| Reuse Status | Reuse restricted to vendor |

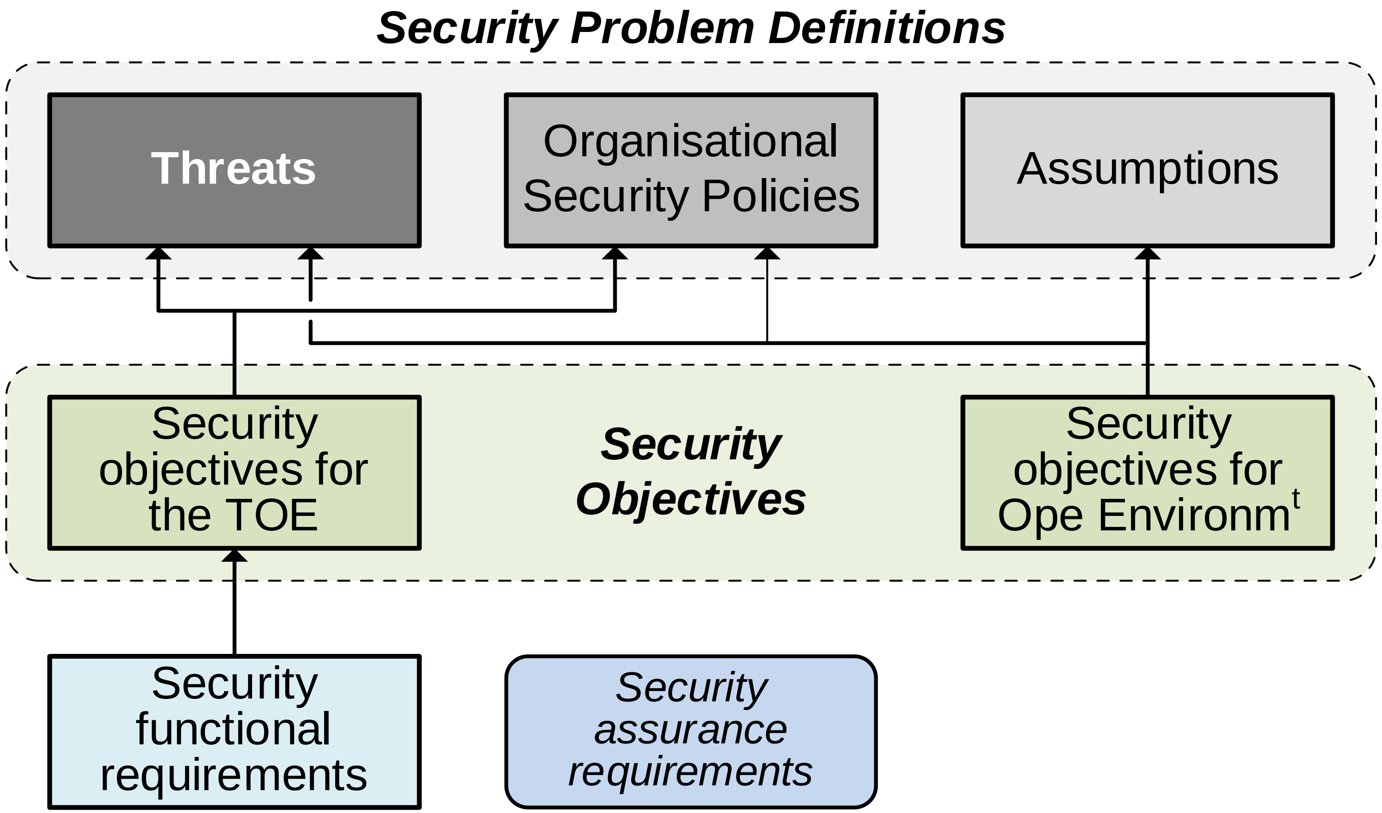
| | Operating Environments | Vetted Conditioning Component CAVP Certificates |
|---|---|---|
| Entropy Per Sample: 1.75 bits<br>Sample Size: 2 bits | • IDQ20MC1<br>• IDQ20MC1-S1<br>• IDQ20MC1-S3<br>• IDQ250C2<br>• IDQ250C3<br>• IDQ6MC1 | |

# AIS31

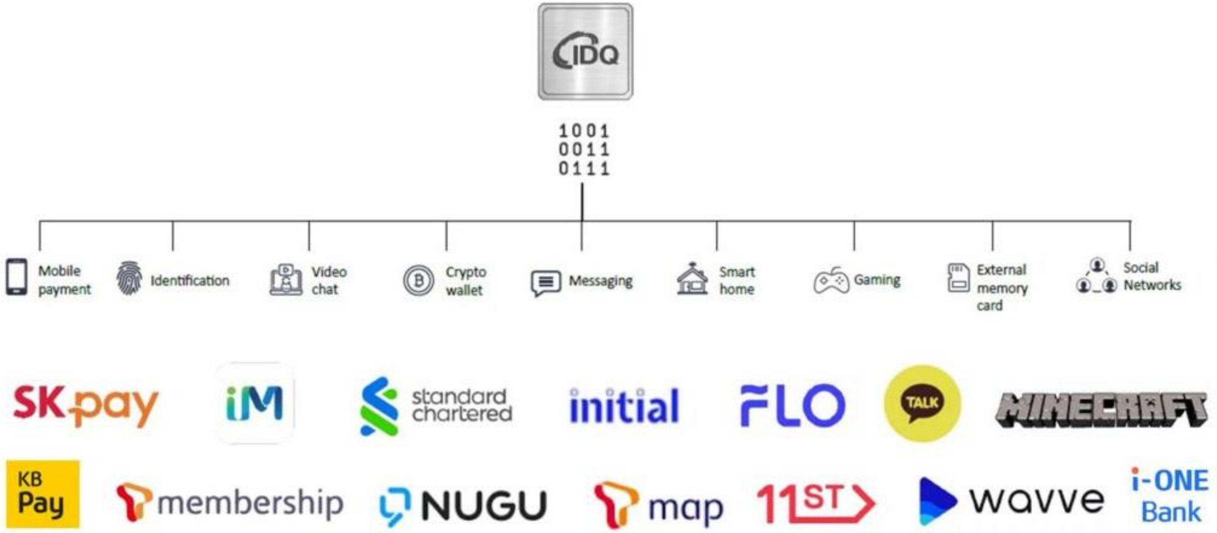


- IDQ’s QRNG has been designed to be PTG.3 compatible
- AIS31 evaluation are done in the Common Criteria framework

# Entropy Validation


Security Problem Definitions
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security Objectives
Security objectives for Ope Environmt
Security functional requirements
Security assurance requirements

# Use Cases



- Mobile payment
- Identification
- Video chat
- Crypto wallet
- Messaging
- Smart home
- Gaming
- External memory card
- Social Networks

# Use Cases

IDQ

20 YEARS QUANTUM INNOVATION

# THANK YOU.