DocuSign®

DocuSign QSCD Appliance

Version 1.0

SP 800-90B Non-Proprietary Public Use Document

Quantis IDQ6MC1 QRNG Chip

Level 3 Validation

July 2023
Document Version 1.0

Table of Contents

List of Figures

1 Revision History

Version	Date	Description
1.0	Jul 23, 2023	Update for v1.2.0.6

2 Definitions

Term	Meaning
ADC	Analog to Digital Converter
API	Application Programming Interface
APT	Adaptive Proportion Test
CIS	CMOS Image Sensor
CMOS	Complementary Metal Oxide Semiconductor
DRBG	Deterministic Random Bit Generator
FIFO	First In First Out
IDQ	Swiss company ID Quantique
IID	Independent and Identically Distributed
LDO	Low-Dropout Regulators
LED	Light Emitting Diode
NRBG	Non-deterministic Random Bit Generator
OVD	Over Voltage Detection
QRNG	Quantum Random Number Generator
RCT	Repetition Count Test
SPI	Serial Peripheral Interface
UVD	Under Voltage Detection

3 Description

The entropy source used within the DocuSign QSCD Appliance (used in conjunction with a HMAC_DRBG) is the high-quality, hardware-based chip (Quantis IDQ6MC1). It is physical noise source (P) that meets the requirements of NIST SP 800-90B (Recommendation for the Entropy Sources Used for Random Bit Generation). The chip generates a seed that is input into the QSCD Appliance approved HMAC_DRBG.

IDQ's patented quantum random number generator (QRNG) chip exploits the fact the number of photons emitted by a common light source fluctuates randomly. These fluctuations, also called "quantum shot noise", are purely of a quantum origin, and are therefore fundamentally random as per the laws of physics.

The structure of IDQ6MC1 QRNG is based on a light emitting diode (LED) and a CMOS image sensor (CIS) pixel array that are respectively integrated inside a QRNG chip as a light source and a multipixel photon detector. All pixel outputs are digitized by a single analog-digital converter (ADC). Based on these ADC output values, the number of detected photons per pixel, as well as their fluctuations, can be measured. Essentially, the quantum shot noise is directly converted into numbers at the output of the ADC. The passage from quantum randomness to an actual random number is straight forward and by no means affected by other unaccounted (and possibly contriving) physical processes that could increase predictability and thwart security.

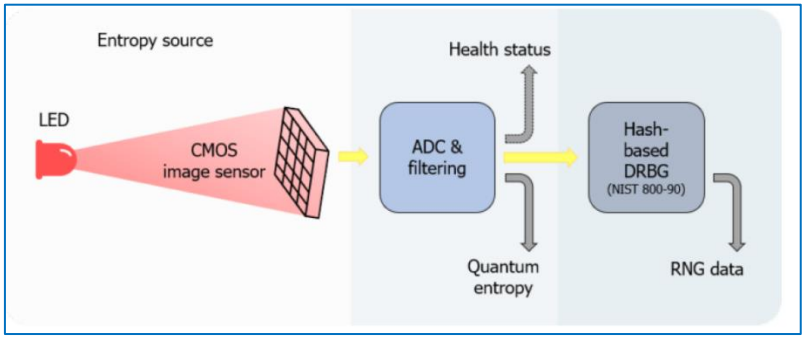

Figure 1 – Structure of IDQ6MC1 QRNG chip

The entropy source is based on physical properties of quantum shot noise of a light source. The non-IID entropy estimation track is chosen.

The entropy source has been tested on DocuSign QDCD Appliance on two operational environments:

- Hardware version 2.0.0.0, Firmware version 1.1.0.9
- Hardware version 2.0.0.0, Firmware version 1.2.0.6

4 Security Boundary

The security boundary of the entropy source is defined by the physical boundary of the IDQ6MC1 chip (shown in Figure 1 above), located on the QSCD tamper board. The IDQ6MC1 chip is covered by a metal shield, which makes it possible to neutralize signal injection attacks and block the leakage of side information.

The IO pins of the chip and the physical lines between the chip and QSCD host processor are securely placed in the QSCD tamper board and the interfaces between the chip and the QSCD host device are all physically protected by the QSCD appliance's tamper protection mechanism.

The basic operations of it such as power-up, data extraction and statistical testing are managed by QSCD's host driver.

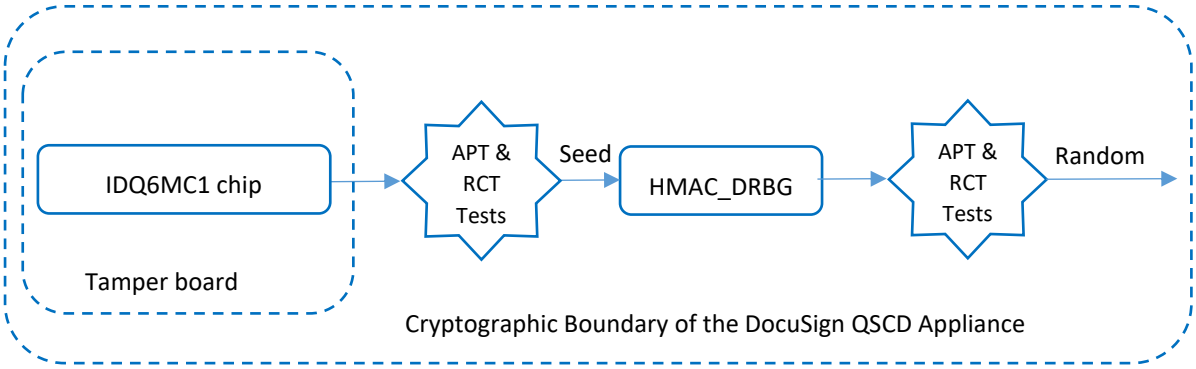

Figure 2 – Cryptographic Boundary of QSCD

5 Operating Conditions

The IDQ6MC1 has passed the AEC-Q100 test and the normal operation with high entropy will be guaranteed by the manufacturer to be –20°C to 85°C. When operating inside the QSCD Appliance, this range is further reduced to +5°C to +45°C (test results are provided for this temperature range).

The operating voltage of the chip inside QSCD Appliance is +2.8v DC ±4%. The external power grid voltage (220vAC 60Hz or 110vAC 50Hz) is converted by the power supplies to +5v DC. The +5v DC voltage is supplied to the QSCD motherboard, tamper device and all other components. Inside the tamper device there is another DC converter from +5v to +2.8v and this voltage is supplied to the IDQ6MC1 chip. The +2.8v converter will shut down if it is unable to supply the required +2.8v, thereby guaranteeing a stable +2.8v DC to the IDQ6MC1 chip.

In addition, the chip includes two internal LDOs (Low-Dropout Regulators) that are used for 1.5v and 1.8v power supply respectively and OVD (Over Voltage Detection) and UVD (Under Voltage Detection) functions are built-in to detect the abnormal voltage input.

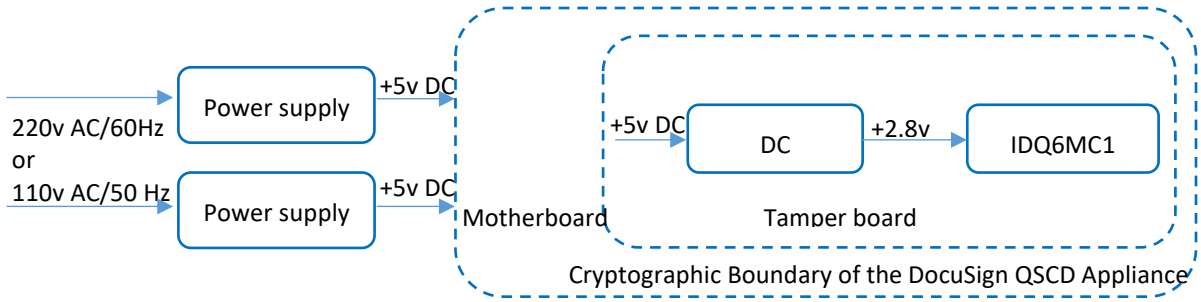

Figure 3 – QSCD Power Supply

Environmental and operating condition's fluctuations (e.g. temperature, voltage or current), can affect the optical power, the LED's brightness, pixel's sensitivity and the ADC output values. Fortunately, the auto-calibration of the chip internal power keeps the entropy maximal even in their presence. A health check function inside IDQ QRNG chips is always monitoring the brightness level. If it is too high or too low beyond the max and min thresholds, then the auto-calibration will start to re-calibrate for setting the brightness level again into the normal range.

6 Configuration Settings

IDQ6MC1 supports two serial interfaces SPI and I²C. This is selected by a hardwired pin configuration. In the QSCD appliance, the SPI interface is used and the IDQ6MC1 chip is operated in the sample mode. This means that the quantum entropy (sample noise) interface of IDQ6MC1 is used without the conditioning function of the chip. The entropy is not mixed by the chip internal hash-based DRBG and instead, the QSCD appliance operates its own health test functions and DRBG mechanism. According to the definitions in the NIST SP800-90B, IDQ6MC1 plays a role of a noise source, not of an entropy source, since IDQ6MC1 provides only raw entropy bits and the health tests are done in a QSCD's host driver.

Upon power-up, a special initialization sequence of commands is sent by the host driver to the IDQ6MC1 chip and prepares it to production of raw entropy data. Also, an internal auto calibration function is activated inside the chip hardware. It controls the optical power supplied by the LED as well as the exposure time of the CIS to keep the entropy maximal in all operating conditions.

7 Physical Security Mechanisms

The physical security mechanisms of the IDQ chip include a metal shield, which makes it possible to neutralize signal injection attacks and block the leakage of side information.

In addition, the chip is located within the tamper-proof and tamper-evident QSCD Appliance. The appliance is encased within a steel box rigged with tamper-responsive micro-switches, and a tamper-evident can that covers a screw joining the top and bottom of the enclosure. Intrusion attempts cause power to be instantly cut off, preventing access to any useful information by zeroizing all plaintext Critical Security Parameters (CSPs). All vents on the module are baffled to meet FIPS 140-3 physical security requirements for opacity and probing.

8 Conceptual Interfaces

The QSCD appliance firmware supports the GetNoise interface. The API of the IDQ6MC1 is used to read raw random data through its SPI interface.

Figure 4 (below) shows the basic step of data extraction. The two-bit samples of raw entropy that are produced by the ADC in each frame, fill bytes in a FIFO register. This register can be accessed by the chip external interface.

The output data packets are treated in the unit of byte, that is, the output space of the noise source is a sequence of bytes (8 bits) with values 0 ~ 255.

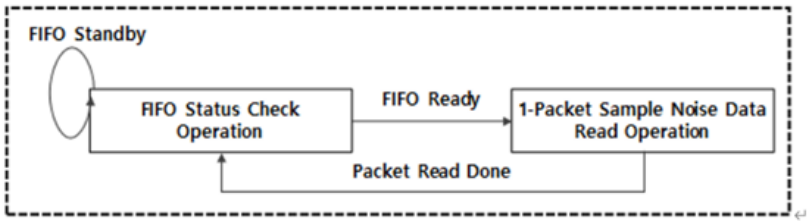

Figure 4 – Noise data access flow

The host driver first checks the FIFO ready register status. If it indicates that the FIFO contains newly generated raw entropy data, it issues a read command to get complete bytes of random data. Each call to get random command collects 16 bytes of raw random data. The code checks that the format of the output data is correct to verify it is a valid data frame and only then, it is checked by the RCT and APT.

If there are no errors in the read operation, raw random data is returned. In case of error, several attempts to read data from the chip are performed and if they all fail, a critical DRNG error is reported, the QSCD services are stopped, and the appliance enters error state.

Data collection does not interfere with the noise source as these are two separate and independent processes that are handled by the chip hardware. The first process is the filling of the FIFO register with entropy data from the noise source. The second process is reading information from the FIFO by calling the external chip API.

9 Min-Entropy Rate

The min-entropy rate at the output of source (as defined by H in section 3.1.4.2 of 90B when there is no conditioning function) for a 2-bit output is:

- Firmware v1.1.0.9: 1.767981 at +15°C
- Firmware v1.2.0.6: 1.760755 at +20°C

Based on the physical model and statistical analysis, the submitter's entropy is set by $H_{submitter}$ = 1.96 (= 0.98 x 2). However, the non-IID test and the restart test will give lower scores, as seen above.

10 Health Tests

The NRBG component passes these types of health tests:

- Power-up self-tests
- Continuous self-tests
- On-demand self-tests

10.1 Power-up Self Tests

Upon power-up, the QSCD services are started and the power-up self -tests are performed by the QSCD firmware. First the QSCD tests the communication with the tamper device. Failure to communicate with the tamper board will result in tamper hardware error and the appliance will enter error state.

Then, the NDRBG is initialized by sending the IDQ6MC1 chip a sequence of initialization commands. The IDQ6MC1 starts the automatic calibration on the analogue components of the chip. It checks the status of LED and CIS and maintains the ADC outputs in the middle of the output range by adjusting LED brightness and CIS exposure time. If the chip fails to adjust the analogue components and does not work properly, then it goes into total failure state and the QSCD appliance enters error state.

And finally, a power-up self-test is performed by the QSCD firmware. The code reads approximately 4000 bytes from the chip and runs the continuous health tests as required by NIST SP 800 90B, section 4.3.4. These random bytes are discarded and only then, random data can be collected from the NRBG.

If any of the power-up self-tests fail, the appliance enters error state, and a corresponding error is displayed. The appliance does not start and no cryptographic services are available.

10.2 Continuous Tests

The QSCD device supports 2048, 3072 and 4096-bit RSA keys. According to Table 2 in NIST SP 800-57 Part 1 Rev 4 (Recommendation for Key Management, Part 1: General), when supporting 4096-bit RSA keys, then a minimum entropy of 192 bits is required (256 x 1.5/2 bits = 192 bits). Therefore, the minimum entropy received from NRBG should be at least H = 1.5.

The output from the hardware-based entropy source (IDQ6MC1 chip) is constantly tested by the following tests:

- Repetition Count Test as defined in NIST SP 800-90B, section 4.4.1, with the following values: $H = 6$, $\alpha = 2^{-30}$, $C = 21$
- Adaptive Proportion Test as defined in NIST SP 800-90B, section 4.4.2, with the following values: $W = 512$, $H = 1.5$, $\alpha = 2^{-30}$ and $C = 248$. The cutoff value C meets the requirement $C <= W$.

If the continuous random tests fail, the appliance enters error state, and a corresponding error is displayed. The appliance stops processing any requests, all services are stopped and the appliance reboots.

10.3 On-Demand Self Tests

It is possible to perform on-demand self-tests by restarting the appliance. The samples collected during on demand health-tests are discarded.

10.4 Error Handling

In case there was failure to communicate with the tamper board and get a new random seed, failure to communicate with the IDQ chip or failure in any of the continuous random tests (RCT and APT) the appliance enters error state, displays a corresponding error and stops processing any requests. All services are stopped and the appliance reboots.

In addition, inside the IDQ6MC1 chip there are two LEDs. One is standby and IDQ6MC1 immediately switches to it if the active one is damaged during operation. Therefore, the IDQ6MC1 can continue to work even when one LED does not work, and it hardly goes into the total failure.

11 Required Testing

The tests below show the results of running the NIST entropy assessment on non-IID data sources (https://github.com/usnistgov/SP800-90B_EntropyAssessment).

Statistical testing was performed across the expected operational temperature range (+5°C to +45°C) of the device to demonstrate the noise source's performance does not degrade. The physical construction of the noise source does not allow for any other testing methodology to be done.

The Entropy Source's compliance to SP 800-90B was validated using the testing interface (not available outside of test units) and the SP 800-90B entropy assessment tool. The entropy source does not expose interfaces to the consuming application (not available in production) and therefore to validate the theoretical assumptions about the noise source and whether it is operating correctly, the consuming application must reply on the status of the health tests as well as through the following tests performed.

Data was collected from the device in its designated operational range and the tests were performed according to Section 3 of SP 800-90B:

- Raw Noise samples comprising of at least 1,000,000 bits were collected via the raw noise source interface and processed by the NIST SP800-90B tool. The entropy rate must approach the min-entropy rate defined in the 'Min-Entropy Rate' Section.

- Restart data must be collected in accordance with the procedure specified in SP800-90B (in the format of 1,000 samples from 1,000 restarts) through the raw noise source interface and processed by the NIST SP800-90B tool. The restart sanity tests must all pass and the minimum of the row-wise and column-wise entropy rate should not be less than half of the entropy rate obtained from the raw noise data test, described above.

No further testing is required on the Entropy Source.