
# अनंतिम टेस्ट गाइड
# टीईसी ९१०२१:२०२५

# PROVISIONAL TEST GUIDE
# No. TEC 91021:2025

---

## for

## क्वांटम यादृच्छिक संख्या जनरेटर

## Quantum Random Number Generator

(STANDARD No.: TEC 91020:2024)

ISO 9001:2015

---

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीद लाल भवन, जनपथ, नई दिल्ली-110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

**Release 1: November, 2025**

# FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of the Department of Telecommunications (DoT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centres (RTECs) have been established, which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

# ABSTRACT

This Test Guide provides detailed test schedules and test procedures for evaluating conformance of the product against Standard on Generic Requirements (GR) for the Quantum Random Number Generator (STANDARD No.: TEC 91020:2024).

# CONTENTS

# A. History Sheet

| S.No. | Standard No. | Title | Remarks |
|---|---|---|---|
| 1. | TEC No. 91021:2025 | Test Guide for Quantum Random Number Generator | Release - 1 November, 2025 |

# B. Introduction

This document describes the test guide for the validation of conformance of the product against Standard on Generic Requirements for the Quantum Random Number Generator (STANDARD No.: TEC 91020:2024).

The manufacturer shall offer his system for type approval along with the following documents:

i. System specifications of the equipment containing features, facilities, and physical description,
ii. Manual for the System, Installation, and Operation & Maintenance of the equipment,
iii. Hardware, Software, and firmware details of the equipment,
iv. Bill of material,
v. Block schematic diagram and physical configuration of the equipment,
vi. Test Results as per the TEC Test Guide of the Standard.

All the necessary set-ups & measuring instruments shall be provided by the manufacturer or by a designated lab (if available) for testing. The manufacturer or lab shall provide proper operating environment for testing.

Note: Though every care has been taken to cover all the parameters of the GR correctly in this Test Guide, yet to avoid any inadvertent error/ misprint, the testing officer shall ensure that all the parameters of the GR have been tested & verified in accordance with the provisions of the GR.

## C. General information for type approval against GR

| S.No. | General Information | Details<br>*(To be filled by testing team)* | | | |
|---|---|---|---|---|---|
| 1 | Name and Address of the Applicant | | | | |
| 2 | Date of Registration of Application | | | | |
| 3 | Name and No. of TEC Standard against which the approval sought | TEC standard No: 91020:2024 | | | |
| 4 | Type of the product | Network Appliance QRNG | Portable QRNG with USB interface | QRNG with PCIe interface | Chip-based QRNG |
| | | | | | |
| 5 | Type of Quantum Entropy Source | QES1 source/ QES2 Source | | | |
| 6 | Quantum Phenomenon | Optical / Non-Optical | | | |
| 7 | Fundamental Source of Quantum Randomness | | | | |
| 8 | Details of | Model No. | Serial No. | | |

| | | | |
|---|---|---|---|
| | Equipment | | |
| | | | |
| 9 | Date of commencement of Tests | | |
| 10 | Place of Testing | | |
| 11 | Any other relevant information | | |
| | … | | |

## D. Testing team

(a) TEC Representatives:

| S.No. | Name | Designation | Organisation | Signature |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| .. | | | | |

(b) Manufacturer's Representatives:

| S.No. | Name | Designation | Organisation | Signature |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| .. | | | | |

## E. List of the Test Instruments

| S.No. | Name of the test instrument | Make /Model | Validity of calibration (upto dd/mm/yyyy) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## F. Equipment Configuration Offered

(a) <Equipment/product name> Configuration:

| S.No. | Item | Details | Remarks |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| .. | | | |
| .. | | | |
| .. | | | |

*Relevant information like No. of cards, ports, slots, interfaces, size, etc. may be filled as applicable for the product.*

(b) <Other equipment > Configuration:

| S.No. | Item | Details | Remarks |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| .. | | | |
| .. | | | |
| .. | | | |

## G. Equipment/System Manuals

| S.No. | Item | Status of availability (Yes/No) | Remarks |
|---|---|---|---|
| 1. | Availability of Installation Manual | | |
| 2. | Availability of User Manual | | |
| 3. | Availability of Maintenance & Repair Manual | | |

## H. Clause-wise Test Type and Test Case No.

| GR Clause No. | Content of the GR Clause | Test Case No. |
|---|---|---|
| | CHAPTER 1 | |
| | Technical Requirements | |
| 1.1 | Introduction to QRNG: | |
| 1.1.1 | This document describes the generic requirements and specifications for Quantum Random Number Generator. | This is for information purpose. |
| 1.1.2 | Random number generators (RNGs) are crucial in many fields, particularly in cryptography, where it is essential for generating secure encryption and decryption keys. Predictable random numbers can lead to potential backdoor attacks, compromising security. It is, therefore, imperative to use a high entropy source RNG, based on quantum phenomenon, to generate true random numbers. Unlike classical processes, quantum processes are fundamentally unpredictable, making the numbers generated from a quantum source intrinsically random and non-deterministic. | This is for information purpose. |
| 1.1.3 | Properties of Random Number Generator<br>(i) Uniformity: There should be equal probability for the occurrence of 0's and 1's at any point of random sequence generation i.e. the expected number of 0's and 1's in the sequence should be equal.<br>(ii) Scalability: The randomness should be retained for any sub-sequences extracted randomly from the generated sequence.<br>(iii) Consistency: The random number generator should behave consistently regardless of the input or time.<br>(iv) Forward secrecy: It refers to the inability to predict future | This is for information purpose. |

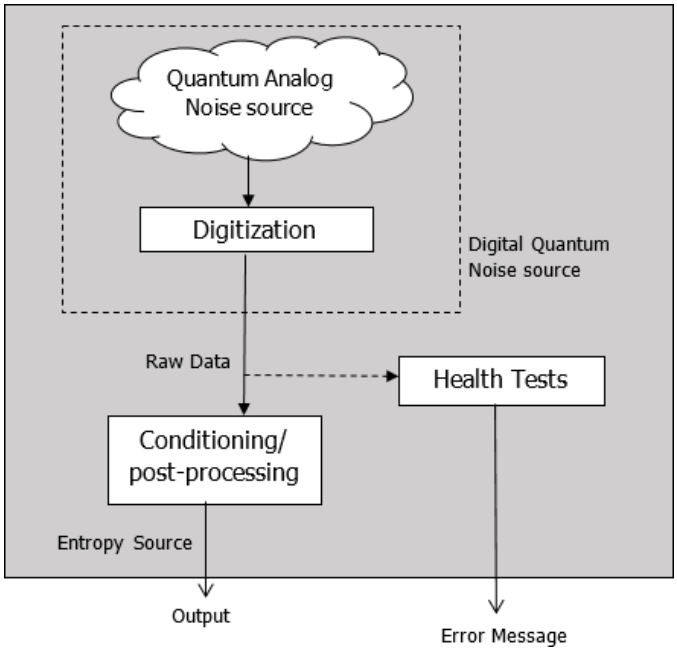
| | | |
|---|---|---|
| | output of the RNG based on the knowledge of previous output values and/or internal states.<br>(v) Backward secrecy: It refers to the inability to determine prior output of an RNG, given knowledge of the current or any future output of the RNG.<br>(vi) Stability: It refers to the ability to produce a stable random sequence over a long period, without being disturbed by the environment. | |
| 1.2 | **Classification of Random Number Generators** | |
| 1.2.1 | Pseudo Random Number Generators (PRNG): Pseudo Random Number Generators, also known as Deterministic Random Bit Generator (DRBG), use algorithms or mathematical functions to produce sequences of random numbers. PRNGs generate a sequence of numbers that approximate the properties of random numbers. A PRNG starts from an arbitrary starting state using an initial seed. PRNGs can generate random numbers at high speeds, however, they have the disadvantage of being reproducible if the seed is known. | This is for information purpose. |
| 1.2.2 | Physical True Random Number Generators (PTRNG): PTRNGs produce high entropy random numbers from a physical noise source based on a randomness-exhibiting physical phenomenon. This phenomenon may be realized by a physical experiment or by an electronic circuit. | This is for information purpose |
| 1.2.3 | Non-Physical True Random Number Generators (NPTRNG): NPTRNGs generate 'true' random numbers, but unlike PTRNGs they do not employ dedicated hardware designs or physical experiments as noise sources. Instead, NPTRNGs prevalently exploit non-physical noise sources such as system data (timing values, RAM data, etc.) or human interaction (key board and mouse events, etc). | This is for information purpose |

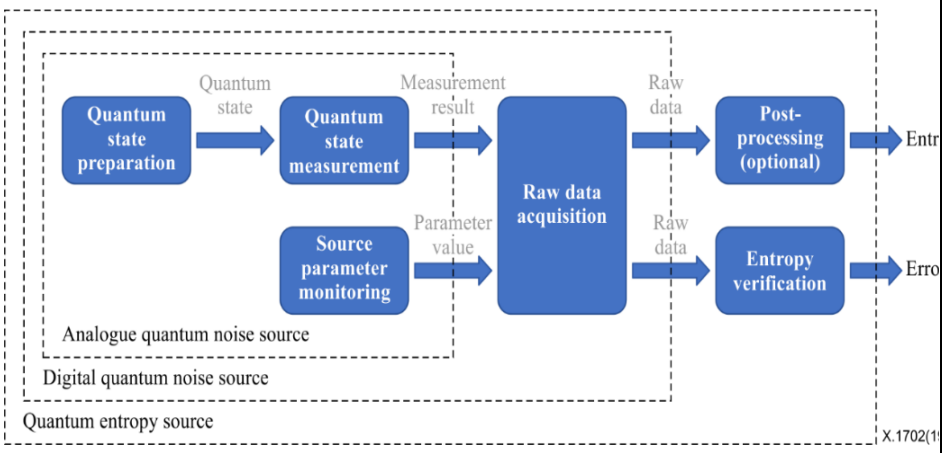
| | | |
|---|---|---|
| 1.2.4 | Based on the phenomenon used, True Random Number Generators can be classified as:<br>(i) Classical TRNG: These rely on classical physics phenomena such as Raman scattering, Clock Jitter, etc. to generate random numbers. The chaotic source of classical randomness is susceptible to initial conditions and thus, could be exploited.<br>(ii) Quantum Random Number Generator (QRNG): QRNG generates random numbers using the principles of quantum physics. Unlike PRNGs which rely on deterministic algorithms and classical TRNGs which depend on chaotic physical phenomena, QRNGs leverage the inherent randomness of quantum phenomena. These devices typically utilize properties like the uncertainty principle, superposition, entanglement, etc. to produce unpredictable sequences of numbers. | This is for information purpose |
| **1.3** | **Fundamental Sources of Quantum Randomness** | |
| 1.3.1 | Quantum physics provides randomness with inherent unpredictability by exploiting the fundamental indeterminism of quantum experiments. | This is for information purpose |
| 1.3.2 | The quantum phenomena include quantum state superposition, quantum state entanglement, Heisenberg uncertainty, quantum tunnelling, spontaneous emission or radioactive decay, etc. The quantum phenomena used for random number generation may be classified as:<br>(i) Optical Quantum Phenomenon:<br>- Branching path, eg. photons from a single photon source or photons from an anti-bunched or sub-Poissonian source passed through a semi-transparent mirror or beam splitter.<br>- Time of arrival of photons<br>- Amplified spontaneous emission<br>- Photon counting<br>- Phase noise of a single-mode laser | Check the type of Quantum Phenomenon declared by the manufacturer and verify the same by inspecting the components, layout and the corresponding datasheet. The observations may be recorded |

| | | |
|---|---|---|
| | - Spontaneous parametric down-conversion leading to binary phase state selection in a degenerate optical parametric oscillator.<br>- Fluctuations in vacuum energy measured through homodyne detection.<br>- EPR Entanglement of field quadratures of multi-mode squeezed light generated by spontaneous four wave mixing (SFWM) and/or spontaneous down conversion (SPDC)<br>- Any other methods using Optical Quantum phenomena, not covered above.<br>(ii) Non-Optical Quantum Phenomenon:<br>- Shot noise, a quantum mechanical noise source in electronic circuits.<br>- Spin noise in atomic systems.<br>- Radioactive decay.<br>- Quantum Tunnelling eg. amplification of the signal produced on the base of a reverse-biased transistor. The emitter is saturated with electrons and occasionally they will tunnel through the bandgap and exit via the base.<br>- Quantum Interference, where the probability amplitude of different quantum states superpose, leading to redistribution of probability density.<br>- Any other methods using Quantum phenomena, not covered above. | |
| **1.4** | **Applications of QRNG** | |
| 1.4.1 | Quantum-secure Cryptography: Random numbers are crucial for creating secure cryptographic keys. QRNGs can be used to generate truly random numbers that can be used to create unbreakable cryptographic keys for secure communication. | This is for information purpose |
| 1.4.2 | V2X Security: QRNG can be used to secure vehicle-to-everything (V2X) communications, ensuring the privacy and | |

| | | |
|---|---|---|
| | safety of connected vehicles. | |
| 1.4.3 | Online Gaming: Random numbers are essential in the gaming industry for creating fair and unbiased games. QRNGs can be used to generate truly random numbers for games such as lotteries, online casinos, and other gambling applications. | |
| 1.4.4 | Mobile Phones: With QRNG chip embedded in mobile phone, enhanced security can be applied to any service and any app on the phone. The QRNG chip adds an additional layer of authentication, boosting security by generating truly unpredictable and random numbers that are used for encryption. | |
| 1.4.5 | Telecommunications: QRNGs can be used in LTE/5G authentication centre (AuC) and other network functions to ensure quantum-safe security. | |
| 1.4.6 | Data Centres: QRNGs can be used for securing data at rest in data centers by providing a source of true randomness for cryptographic operations. This can be used to generate strong encryption keys, randomize data, and create unique identifiers for data elements. | |
| 1.4.7 | Tokenization: Tokenization is crucial for securing and masking customer data, especially in the banking sector. With the rise in digital adoption, the demand for tokens has increased, leading to repetition and correlation in token generation. QRNG can be used to generate random tokens. | |
| 1.4.8 | Exams and Certifications: QRNG can be used to generate unique identifiers and randomize exam questions, preventing cheating and ensuring fairness. | |
| 1.4.9 | Simulation and Modelling: In many scientific applications, truly random numbers are needed to simulate natural phenomena, such as the weather, the behavior of materials, and biological systems. QRNGs can provide a source of truly random numbers | |

| | | |
|---|---|---|
| | for these simulations | |
| 1.4.10 | Statistical analysis: Random numbers are essential in statistical analysis, for example, in Monte Carlo simulations, where random numbers are used to generate samples for statistical analysis. QRNGs can provide a source of truly random numbers for these types of applications. | |
| **1.5** | **Types of QRNG** | |
| 1.5.1 | The QRNG can be offered in various form factors, categorized as below<br>1. Network Appliance QRNG<br>2. Portable QRNG with USB interface<br>3. QRNG with PCIe interface<br>4. Chip-based QRNG | Indicate the category of QRNG offered for testing in Table C of this test guide. |
| **1.6** | **Functional Architecture of Quantum Entropy Source** | |
| 1.6.1 | In random number generation, ensuring true randomness is crucial for security, reliability, and fairness in various applications like cryptography, simulations, and gaming. Quantum entropy sources provide randomness based on natural phenomena that are inherently unpredictable. Unlike pseudo-random algorithms, which are deterministic and potentially vulnerable to prediction, quantum entropy sources offer randomness that resists cryptographic attacks and ensures unbiased outcomes. It enhances the integrity and trustworthiness of systems dependent on random number generation. | This is for information purpose. |

| | | |
|---|---|---|
| 1.6.2 | The high-level block diagram for the entropy source in True Random Number Generator can be represented as below:<br>  <br><br>(i) Noise Source: The noise source is the root of security for the entropy source and for the Random Number Generator as a whole. This is the component that contains the non-deterministic, entropy-providing process that is ultimately responsible for the uncertainty associated with the random numbers output by the entropy source. If the non- deterministic activity being sampled produces something other than binary data, the sampling process includes a digitization process that converts the output samples to bits. The output of the digitized noise source is called the raw data.<br>(ii) Conditioning Component / Post-processing: The optional conditioning component or post-processing is a deterministic function responsible for reducing bias and/or increasing the entropy rate of the resulting output bits (if necessary to obtain a target value).<br>(iii) Health tests: Health Tests are an integral part of the entropy source design that are intended to ensure that the noise | Test Case No. 1 |

| | | |
|---|---|---|
| | source and the entire entropy source continue to operate as expected. When testing the entropy source, the end goal is to obtain assurance that failures of the entropy source are caught quickly and with a high probability. Another aspect of health testing strategy is determining the likely failure modes for the entropy source and, in particular, for the noise source. Health tests are expected to include tests that can detect failure conditions which may include insufficient entropy generation, environmental instability, hardware malfunctions, external interferences, etc. | |
| 1.6.3 | The functional architecture of Quantum Entropy sources in QRNG shall be as per ITU-T Recommendation X.1702 " Quantum noise random number generator architecture".<br>  <br> | The functional architecture of the product shall be submitted by the manufacturer.<br>It shall also include the following details:<br>1. How the quantum states is prepared.<br>2. Method for measurement of quantum states.<br>3. Details of digitization step<br>4. Post-processing components, if supported by QRNG |
| 1.6.4 | A quantum process to generate quantum noise can be decomposed in two steps: a quantum state preparation and a quantum state measurement. The generation of raw data by the Quantum Entropy Source shall include the following functional modules:<br>(i) Quantum state preparation: The quantum state can be optical or non-optical and either remain the same or be different in each iteration.<br>(ii) Quantum state measurement: Applying a measurement basis | |

| | | |
|---|---|---|
| | to the propagated state or the state derived from the quantum state preparation.<br><br>NOTE – The combination of the 'quantum state preparation' module and the 'quantum state measurement' module composes an analogue quantum noise source.<br><br>(iii) Raw data acquisition: This step is to generate raw data from quantum state measurement results. A digitization step is needed if the quantum state measurement results are analogue.<br><br>(iv) Post-processing/ Randomness Extractor (optional): In some cases, the raw data might be post-processed before being output as entropy source output. One of the main reasons is most QRNG sources output is a mixture of both classical and quantum noise.<br><br>Depending on the number of functional steps used for the description of the quantum entropy source, the entropy source can output either the raw data generated by the 'raw data acquisition' step, or the output from the 'post- processing' step | |
| 1.6.5 | The entropy estimation of quantum noise sources is based on ideal models that are difficult to implement perfectly. In most cases, the entropy of a quantum noise source is partly due to the relevant quantum process and some additional physical noise coming from implementation imperfections. It is possible for most quantum noise sources to estimate the entropy solely due to the relevant quantum process. | This is the clause of GR for information purpose only |
| 1.6.6 | Quantum entropy sources can be classified in two subclasses depending on their means of entropy estimation. One subclass of quantum entropy source will assess a given minimum entropy amount by measuring the implementation imperfections and | Indicate the type of QES offered for testing in Table C of this test guide. |

| | | |
|---|---|---|
| | verifying that they are within defined acceptable value ranges. This subclass of quantum entropy sources (QESs) is called QES1. Another subclass of QESs, called QES2, will directly assess their entropy amount by measuring signatures of the quantum process. Then, in both cases, by using an appropriate randomness extractor, it is possible to create an output whose entropy arises solely from the considered quantum process. | |
| 1.6.7 | The description of a quantum entropy source shall include the definitions of the conditions (e.g., environmental constraints) under which this description remains valid.<br>(i) In the case of QES1 sources, these conditions are required to include at least:<br>- the noise arising from implementation imperfections; and<br>- the range over which the value of this noise can vary<br>(ii) In the case of QES2 sources, these conditions are required to include at least:<br>- the signature(s) of the quantum process; and<br>- their acceptance range used to assess the entropy of the quantum source under evaluation and to ensure the continued working of the components of the system. | Depending upon the type of entropy source the conditions for which the description of quantum entropy source remains valid shall be provided as per the clause. |
| 1.6.8 | The description of the quantum state preparation and measurement modules is required to rely on quantum formalism. | Already covered in test details pertaining to clause 1.6.4 |
| 1.6.9 | A method of estimation of the entropy generated by the quantum entropy source under evaluation is required to be based on the description of the source. This estimation is recommended to be based on quantum information theory or other approved | The information shall be submitted by the manufacturer |

| | | |
|---|---|---|
| | methods related to quantum physics. | about how the entropy is estimated. |
| 1.6.10 | Entropy Assessment: The QRNG shall carry out the assessment of the entropy generated by the Quantum process and carried by the raw data by a three-step process as below:<br><br>(i) Source parameter monitoring: A source parameter monitoring function is required to monitor the conditions under which the raw data is generated by the digital entropy source.<br><br>(ii) Raw data acquisition: The source parameters are digitized and added in the flow of raw data. These source parameters will not be used to generate the output flow of the entropy source but to verify its entropy.<br><br>Note: The raw data is composed of the bit sequence ('measurement result') and additional digital values ('parameter value', e.g., temperature, voltage, tampering attempts etc.) generated by the entropy source.<br><br>(iii) Entropy verification: The raw data will be processed in order to verify if the entropy generated by the digital quantum noise source is at least higher than the minimum entropy amount specified. | Test Case No. 2 |
| 1.7 | Requirements for Quantum Entropy Source | |
| 1.7.1 | The entire design of the Quantum entropy source shall be documented, including the interaction among the various components | The manufacturer shall submit the functional block diagram of the QES indicating all |

| | | |
|---|---|---|
| | | the components used. |
| 1.7.2 | Documentation shall describe the operation of the Quantum entropy source, including how the Quantum entropy source works, and how to obtain data from within the Quantum entropy source for validation testing | Applicable documentation shall be submitted by the manufacturer |
| 1.7.3 | Documentation shall describe the range of operating conditions (e.g., temperature range, voltages, system activity, etc.) under which the Quantum entropy source is claimed to operate correctly. | |
| 1.7.4 | The Quantum entropy source shall have a well-defined (conceptual) security boundary. This security boundary shall be documented; the documentation shall include a description of the content of the security boundary. | The documentation describing the physical and logical security boundaries of the QRNG shall be submitted by the manufacturer. |
| 1.7.5 | When a post-processing component is not used, the output from the Quantum entropy source is the output of the noise source, and no additional interface is required. | Test case No. 3 |
| 1.7.6 | When a post-processing component is included in the Quantum entropy source, the output from the Quantum entropy source is the output of the post-processing component, and an interface is required to access the quantum noise-source output. In this case, the quantum noise-source output shall be accessible via the interface during validation testing, but the interface may be | Test Case No. 4 |

| | | |
|---|---|---|
| | disabled otherwise. The manufacturer shall fully document the method used to get access to the raw Quantum noise source samples. If the noise-source interface is not disabled during normal operation, any noise-source output using this interface shall not be provided to the post- processing component for processing and eventual output as normal Quantum entropy-source output. | |
| 1.7.7 | The Quantum entropy source may restrict access to raw quantum noise source samples to special circumstances that are not available to users in the field, and the documentation shall explain why this restriction is not expected to substantially alter the behaviour of the Quantum entropy source as tested during validation. | Test Case No. 5 |
| 1.7.8 | Documentation shall contain a description of the restarting process applied during the restart tests. | 1. The details of the restart tests shall be submitted by the manufacturer.<br>2. Reboot the QRNG and check the status of the restart tests (pass/fail) through GUI or logs. |

| | | |
|---|---|---|
| 1.7.9 | Documentation shall contain a concrete information theoretical randomness proof using entropic uncertainty relation, universal hash lemma or non- classical inequality, etc. | Applicable documentation shall be submitted by the manufacturer. |
| **1.8** | **Requirements for Quantum Noise Source** | |
| 1.8.1 | The operation of the Quantum noise source shall be documented; this documentation shall include a description of how the Quantum noise source works, where the unpredictability comes from, and rationale for why the Quantum noise source provides acceptable entropy output, basis of randomness and should reference relevant, existing research and literature. | Applicable documentation shall be submitted by the manufacturer. |
| 1.8.2 | The behaviour of the Quantum noise source shall be stationary (i.e., the probability distributions of the Quantum noise source outputs do not change when shifted in time). | Test Case No. 6 |
| 1.8.3 | Documentation shall provide an explicit statement of the expected entropy provided by the Quantum noise source outputs and provide a technical argument for why the noise source can support that entropy rate. To support this, documentation may include a stochastic model of the Quantum noise source outputs, and an entropy estimation based on this stochastic model may be included. | The stochastic model of the Quantum noise source and the entropy estimation based on the model may be submitted by the manufacturer |
| 1.8.4 | The Quantum noise source state shall be protected from adversarial knowledge or influence to the greatest extent | Applicable documentation |

| | | |
|---|---|---|
| | possible. The methods used for this shall be documented, including a description of the (conceptual) security boundary's role in protecting the Quantum noise source from adversarial observation or influence. | shall be submitted by the manufacturer.<br>Further, verify that the user should be authenticated before accessing the data from QRNG. |
| 1.8.5 | Although the Quantum noise source is not required to produce unbiased and independent outputs, it shall exhibit random behaviour; i.e., the output shall not be definable by any known algorithmic rule. Documentation shall indicate whether the noise source produces IID data or non-IID data. If the manufacturer makes an IID claim, documentation shall include rationale for the claim. | Record whether the Quantum noise source produces IID or non-IID data. The rationale for the same is to be submitted by manufacturer. |
| 1.8.6 | The Quantum noise source shall generate fixed-length bitstrings. A description of the output space of the Quantum noise source shall be provided. Documentation shall specify the fixed symbol size (in bits) and the list (or range) of all possible outputs from the quantum noise source. | Applicable documentation shall be submitted by the manufacturer |
| 1.8.7 | An additional noise source may be included if the primary entropy source is insufficiently reliable from a failure perspective. In this case, the additional entropy source shall satisfy the same requirements as the primary noise source. | Test Case No. 8 |

| | | |
|---|---|---|
| 1.8.8 | If additional noise source outputs to increase security are used, a document that describes the additional noise sources shall be included. | |
| **1.9** | **Requirements for the Post-processing** | |
| 1.9.1 | The manufacturer shall document which post-processing (conditioning) component is used and the details about its implementation (e.g., the hash function, cryptographic algorithms, and/or key size used). Documentation shall also include the input and the output sizes, $n_{in}$ and $n_{out}$ of the post-processing component | The manufacturer shall submit post-processing (conditioning) component used with implementation details including the key size, input and output sizes, etc.<br><br>Using CLI, request the bit string with number of bits specified as $n_{out}$ declared by the manufacturer. The QRNG should provide $n_{out}$ bits.<br><br>Using CLI, request the bit string with number of bits specified as not equal to $n_{out}$ |

| | | |
|---|---|---|
| | | declared by the manufacturer. In this case, the QRNG should provide an error or an output truncated to a multiple of $n_{out}$ bits. |
| 1.9.2 | The documentation shall describe how the post-processing component enhances the entropy obtained from the QRNG, ensuring that the output data meets randomness and security standards. | Record the value of entropy before the post-processing and after the post-processing from GUI/CLI. |
| 1.9.3 | If the post-processing component uses cryptographic keys, the keys may be<br>(1) fixed to a predetermined value, (2) set using some additional input to the device, or (3) generated by using the quantum noise source outputs. The key shall be determined before any outputs are generated from the post- processing component. | Record the method of key generation used for the post processing component, if applicable. It shall be verified that key is determined before output generation from post processing component. |
| 1.9.4 | Any value which is used to determine the key shall not be used as any other input to the post-processing component. The input entropy to the post- processing component ($h_{in}$) shall not include any entropy provided to the key of a keyed function. | If the input entropy is used for key generation of post-processing |

| | | |
|---|---|---|
| | | component, the manufacturer shall demonstrate the same using CLI and if not possible, an undertaking may be submitted by the manufacturer. |
| 1.9.5 | For Quantum entropy sources containing a post-processing component that is not specified in NIST SP 800-90B, a description of the post-processing component shall be provided. Documentation shall state the narrowest internal width and the size of the output blocks from the post-processing component. The manufacturer shall provide mathematical evidence that the post-processing component is suitable to be used to condition the Quantum noise source output, and does not significantly reduce the entropy rate of the entropy source output. The manufacturer shall also provide a justification about why the post-processing component does not act poorly when the noise source data is not independent. | The details may be submitted by the manufacturer. |
| 1.9.6 | The post-processing component shall not extend the raw data it receives as input. | Ensure that the output length of the post-processing component ($n_{out}$) declared by the manufacturer is not longer than the input length of the |

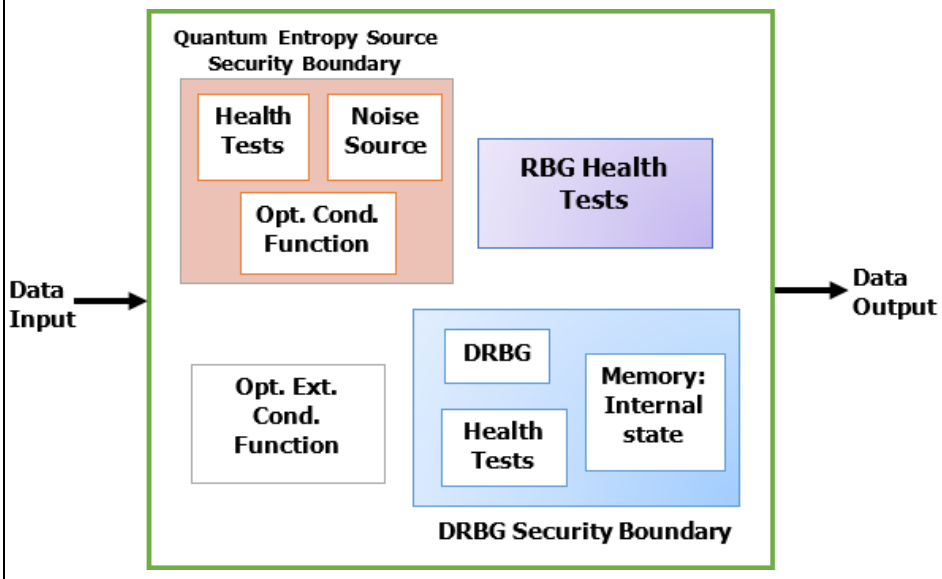
| | | |
|---|---|---|
| | | post-processing component ($n_{in}$) |
| 1.9.7 | The post-processing component, also known as the randomness extractor used to increase the entropy per bit of the source is recommended to be a quantum-proof extractor (optional). | If a quantum-proof extractor is used, the details may be provided by the manufacturer. |
| **1.10** | **Requirements for Health Tests** | |
| 1.10.1 | The health testing of Quantum noise sources shall be done to detect failures of the noise source, based on the expected output during a failure, or to detect a deviation from the expected output during the normal operation of the Quantum noise source. Health tests are expected to raise an alarm,<br>1. When there is a significant decrease in the entropy of the outputs,<br>2. When Quantum noise source failure occurs, or<br>3. When hardware fails, and implementations do not work correctly. | Test Case No. 9 |
| 1.10.2 | Health Tests shall be applied to the outputs of a Quantum noise source before any post-processing is done. | Test Case No. 9 |
| 1.10.3 | Start-up health tests are designed to be performed after powering up, or rebooting, and before the first use of the Quantum entropy source. The start-up test shall be applied immediately after the QRNG has been started. It shall detect a total failure of the Quantum noise source and severe statistical weaknesses. | Test Case No. 9 |
| 1.10.4 | The samples drawn from the Quantum noise source during the start-up tests shall not be available for normal operations until the tests are completed; these samples may be discarded at any | Test Case No. 9 |

| | | |
|---|---|---|
| | time, or may be used after the completion of the tests if there are no errors. | |
| 1.10.5 | Continuous health-tests shall run indefinitely on the outputs of the Quantum noise source while the Quantum noise source is in operation. Continuous tests focus on the behaviour of the noise source and aim to detect failures as the noise source produces outputs. The purpose of continuous tests is to allow the Quantum entropy source to detect any kinds of failures in its underlying Quantum noise source. | Test Case No. 10 |
| 1.10.6 | The continuous health tests shall run continuously on all digitized samples obtained from the Quantum noise source, and so tests must have a very low probability of raising a false alarm during the normal operation of the noise source. | Test Case No. 10 |
| 1.10.7 | The continuous health tests shall atleast include the tests as specified in NIST SP 800-90B. | A self-declaration of conformity shall be submitted by the manufacturer. |
| 1.10.8 | The optimal value for the false positive probability may depend on the rate that the Quantum entropy source produces its outputs. The false positive probability is recommended to be between $2^{-20}$ and $2^{-40}$. Lower probability values are acceptable. The manufacturer shall specify a false positive probability suitable for their application. | Test Case No. 10 |
| 1.10.9 | The Quantum entropy source shall support on-demand health tests. The on- demand tests shall include at least the same testing done by the start-up tests. The entropy source may support on-demand testing by restarting the entropy source and rerunning the startup tests, or by rerunning the startup tests without restarting the entropy source. The manufacturer shall specify the approach used for on-demand testing. | Test Case No. 11 |

| | | |
|---|---|---|
| 1.10.10 | The on-demand tests may include other tests defined by the developer, in addition to the testing done in the start-up tests. | Test Case No. 11 |
| 1.10.11 | Samples collected from the Quantum noise source during on-demand health tests shall not be available for use until the tests are completed; however, these samples may be discarded at any time, or may be used after the completion of the tests providing that there are no errors | Test Case No. 11 |
| 1.10.12 | If a failure of the Quantum entropy source occurs while the QRNG is being operated, the random bit stream shall be disabled immediately, until an appropriate set of health tests confirm resumption of normal operational state of QES. | Test Case No. 12 |
| 1.10.13 | Health tests shall be performed on the noise source samples before any post-processing is done. Additional health tests may be performed on the outputs of the post-processing function. | Test Case No. 9 |
| 1.10.14 | The Quantum entropy source's start-up tests shall run the continuous health tests over at least 1024 consecutive samples. The start-up tests may include other tests defined by the developer. The samples subjected to start-up testing may be released for operational use after the start-up tests have been passed, or may be discarded at any time. | Test Case No. 9 |
| 1.10.15 | When the health tests fail, the Quantum entropy source shall notify the consuming application of the error condition. The manufacturer may define different types of failures (e.g., intermittent and persistent), and the application is allowed to react differently to different types of failures (e.g., by inhibiting output for a short time). The health status may be included as a parameter in response to the request received from an application. Then application can decide whether to use the random numbers. | Test Case No. 9 |
| 1.10.1 | The manufacturer may define different cut-off values to detect | Test Case No. 13 |

| | | |
|---|---|---|
| 6 | intermittent and persistent failures. If so, these values (with corresponding false alarm probabilities) shall be specified in the submission documentation. If the Quantum entropy source detects intermittent failures and allows the Quantum noise source to return to normal functioning, the designer shall provide evidence that: a) The intermittent failures handled in this way are indeed extremely likely to be intermittent failures; and b) the tests will detect a permanent failure when one occurs, and will ultimately signal an error condition to the consuming application and cease operation. In the case where a persistent failure is detected, the Quantum entropy source shall not produce any outputs. The module may support being reset or returned to operation by the consuming application or system. | |
| 1.10.17 | The manufacturer shall provide documentation that specifies all Quantum entropy source health tests and their rationale. The documentation shall include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at power-up continuously, or on- demand), and include rationale indicating why each test is believed to be appropriate for detecting one or more failures in the noise source. | Applicable documentation shall be submitted by the manufacturer |
| 1.10.18 | The manufacturer shall provide documentation of any known or suspected noise source failure modes (e.g., the Quantum noise source starts producing periodic outputs like 101…01), and shall include developer-defined continuous tests to detect those failures. These should include potential failure modes that might be caused by an attack on the device. | Applicable documentation shall be submitted by the manufacturer |
| 1.10.19 | Appropriate health tests that are tailored to the noise source should place special emphasis on the detection of misbehavior near the boundary between the nominal operating environment and abnormal conditions. This requires a thorough understanding of the operation of the noise source. | Documentation regarding thorough operation of the noise source shall be submitted by |

| | | |
|---|---|---|
| | | the manufacturer |
| 1.11 | Other Requirements | |
| 1.11.1 | QRNG shall have an interface for entropy output and another interface for management purpose. | The interface for entropy output and another interface for management purpose shall be verified cloud CLI. |
| 1.11.2 | QRNG shall be compatible with the operating systems. The operating systems supported by the QRNG shall be specified by the manufacturer. | Manufacturer shall provide the OS systems supported in the table given in clause 1.15 |
| 1.11.3 | QRNG shall have a distributed architecture if it supports multiple applications simultaneously. | Declaration to be submitted by manufacturer along with architecture diagram |
| 1.11.4 | QRNG may include an embedded NIST 800-90A approved DRBG along with a physical quantum entropy source, each with its own conceptual security boundary. | Declaration to be submitted by manufacturer if applicable |
| 1.11.5 | The construction of QRNG that includes DRBG mechanism shall be compliant to NIST SP 800-90C. | Declaration along with the compliance certificate |

| | | |
|---|---|---|
| 1.11.6 | For an embedded DRBG, both the quantum entropy source and the DRBG shall contain their own health tests within their respective security boundaries as illustrated below:<br>  <br><br>Figure 3: QRNG Security Boundary as per NIST SP 800-90C (4th Public Draft) | This is the clause of GR for information purpose only |
| **1.12** | **Statistical Testing of Randomness** | |
| 1.12.1 | The sequence at the output of QRNG must pass the following statistical test suites:<br>(i) NIST SP 800-22<br>(ii) Dieharder Tests<br>(iii) ENT Tests<br>(iv) Any other statistical tests, as prescribed. | Test Case No. 14 |
| 1.12.2 | The QRNGs adopting Quantum entanglement in the entropy generation process, shall include a CHSH Bell test. The test shall be defined for discrete variable (DV) or continuous variable (CV) according to the implementation. | Test Case No. 15 |
| **1.13** | **Performance Requirements of QRNG** | |
| 1.13.1 | The validation of the Quantum entropy source may be carried out by the Manufacturer as per NIST SP 800-90B. | A validation certificate to be submitted by the |

| | | |
|---|---|---|
| | | manufacturer |
| 1.13.2 | The QRNG shall deliver output with entropy per data bit very close to 1 with a high level of assurance. The average Shannon entropy and the average min-entropy per raw number bit after algorithmic post-processing (if any) shall exceed 0.9998, and 0.98 respectively.<br>NOTE: The algorithmic post-processing may be applied to the raw random numbers for the purpose of increasing the entropy per data bit (entropy extraction). The entropy measurement shall be made before any Cryptographic post-processing which is the stateful post-processing (i.e., with memory) for the purpose of gaining DRBG security properties (computational security). | Test Case No. 16 |
| 1.13.3 | The statistical properties of the raw random numbers shall not significantly change with the environmental conditions (e.g. temperature, voltage, etc.) | Would be covered with QM-333 testing |
| 1.13.4 | The total failure of the entropy source shall be immediately detectable. A degradation of the entropy source shall be detected sufficiently fast, where “sufficiently fast” depends on the degree of degradation. | Test Case No. 17 |
| 1.13.5 | The system shall raise alarm(s) in case of failures. | Test Case No. 18 |
| 1.13.6 | On detection of an error, the QRNG shall either (a) enter a permanent error state, or (b) be able to recover from a loss or compromise of entropy if the permanent error state is deemed unacceptable for the application requirements. These requirements may be satisfied procedurally or innately in the design. | Covered in Test Case No. 13 |
| 1.13.7 | The software/hardware in the equipment shall not pose any problem due to changes in date and time caused by events such as changeover of millennium/century, leap year etc. in the normal functioning of the equipment. | Test Case No. 19 |

| | | |
|---|---|---|
| 1.13.8 | The QRNG shall have the provision to securely update the firmware. | Test Case No. 20 |
| 1.13.9 | Category-A QRNG shall support simultaneous multiple requests from applications. | Test Case No. 21 along with the Declaration by manufacturer giving the maximum number of simultaneous requests QRNG can handle. |
| 1.13.10 | An interface shall be available to obtain raw, digitized outputs from the quantum noise source. Such an interface shall be available only in “test mode” and it shall be disabled when the source is operational. The test mode may be disabled when QRNG is deployed in the field as per the requirement of the user. | Test Case No. 1 along with disable from the manufacturer |
| 1.13.11 | If the QRNG is capable of operating in more than one mode, the QRNG should return information about the mode in which it is operating, upon request. | Test Case No. 22 |
| 1.13.12 | The QRNG shall supply random numbers through a secure standard interface and provide protection against unauthorized access including the identity authentication of the application. | Test Case No. 23 |
| 1.13.13 | The conditioned or the raw entropy may be delivered to applications/clients over a standard TCP/IP network connection with encryption protocols such as TLS or via mutually authenticated TLS. | Covered in Test Case No. 23 |
| 1.13.14 | The request for random numbers from the entropy output interface shall include the following parameters:<br>- size: Number of random bits requested | Test Case No. 24 |

| | | |
|---|---|---|
| | - source: the source of the random bits (processed or raw)<br>- format (optional): binary, hex, JSON, etc. | |
| 1.13.15 | The message in response to the request from the application shall include the following parameters:<br>- unique ID of the Quantum Entropy Source<br>- random bytes (encoded in base64 for JSON format)<br>- mode (raw or processed random numbers)<br>- timestamp<br>- status (True if the request has been satisfied, otherwise false)<br>- health status | Test Case No. 25 |
| 1.13.16 | An interface may optionally be available to request the entropy source to conduct a test of its health. The request for the health test may include:<br>Input: type of test requested: A bitstring that indicates the type or suite of tests to be performed<br>Output: status: A Boolean value that is TRUE if the entropy source passed the requested test, and is FALSE otherwise. | Already covered in Test Case No. 9,10,11 |
| 1.13.17 | The system shall generate system logs for audit purpose. The logs may be classified with the appropriate labels e.g. Request, Response, warning, Information, Error, Debug, etc. | Test Case No. 26 |
| 1.13.18 | The system shall support secured access along with user management and authentication. | Steps same as Test Case No. 23 |
| 1.13.19 | The management shall be performed through a physical interface, web-based (HTTPS) interface, TLS-protected API calls, or via SSH command line. | Steps same as Test Case No. 23 |
| 1.13.20 | Online Performance Monitoring: The QRNG system shall provide the facility for monitoring of system information and performance parameters. The performance parameters shall include the status of health tests, entropy output per bit, etc. | Test Case No. 27 |
| 1.13.2 | Suitable visual indications shall be provided, to indicate the | Physical Check |

| | | |
|---|---|---|
| 1 | healthy/ unhealthy conditions of the system. | |
| **1.14** | **Security Requirements of QRNG** | |
| 1.14.1 | The QRNG shall not leak relevant secret information (e.g., internal state) through the output. | An undertaking to be submitted by the manufacturer. |
| 1.14.2 | The QRNG shall be resilient against side-channel and fault attacks. | An undertaking to be submitted by the manufacturer. Further, the measures uses to prevent the side-channel and fault attacks shall be provided by the manufacturer. |
| 1.14.3 | The design and implementation of QRNG shall have a defined protection boundary. The protection boundary shall be as specified in ISO/IEC 19790. | The manufacturer shall submit document regarding protection/security boundary and a self-declaration that it is as per ISO/IEC 19790. |
| 1.14.4 | The QRNG design shall include methods to prohibit predictable influence, manipulation, or predicting the output of the QRNG by observing the physical characteristics (e.g., power consumption, timing or emissions). | Test Case No. 28 |
| 1.14.5 | There shall be design evidence (theoretical, empirical, or both) to support all security requirements for the QRNG, including | The details to be submitted by the |

<table>
<tr><td></td><td>protection from misbehavior.</td><td>manufacturer.</td></tr>
<tr><td>1.14.6</td><td>Authentication mechanisms must be used to authenticate an operator accessing the system and to verify that the operator is authorized to access the system.</td><td>Check whether an authentication mechanism (Userid/password) is implemented to access the QRNG system for GUI access and CLI access (user/admin).</td></tr>
<tr><td>1.14.7</td><td>The QRNG shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the system (including substitution of the entire system) when installed. All hardware, software, firmware, and data components within the security boundary shall be protected. [Category-A/B/C/D as applicable]</td><td>Test Case No. 28</td></tr>
<tr><td>1.14.8</td><td>The QRNG shall provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the system is attempted. [Category-A & B]</td><td>Test Case No. 28</td></tr>
<tr><td>1.14.9</td><td>If the QRNG contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure. [Category-A & B]</td><td>Physical Check</td></tr>
<tr><td>1.15</td><td>Technical Specifications of QRNG</td><td></td></tr>
<tr><td></td><td><table>
<tr><th>Details</th><th>Parameters</th><th>Specifications</th></tr>
<tr><td>Type of QRNG</td><td>Category A/B/C/D</td><td></td></tr>
<tr><td></td><td>Source of Quantum</td><td></td></tr>
</table></td><td>Parameters and specifications to be submitted by the manufacturer</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | Entropy Source | Randomness | | |
| | | Type of Quantum Entropy Source (QES1 or QES2) as per clause 1.6.6 | | |
| | | Entropy Estimation of the Quantum Noise Source (as per clause 1.8.3) | | |
| | Performance | Average Shannon Entropy (as per clause 1.13.2) | | |
| | | Average Min-Entropy (as per clause 1.13.2) | | |
| | | Quantum Noise Source Bit Rate | | |
| | | Random post-processed bit rate | Low rate | < 10 Mbps |
| | | | Medium rate | 10 – 100 Mbps |
| | | | High rate | 100 – 1000 Mbps |
| | | | Very high rate | > 1 Gbps |
| | | Number of simultaneous requests supported with key length | | |
| | | Latency - Time delay between request and response from QRNG (in µsec) | | |

| | | | |
|---|---|---|---|
| Compliance | NIST SP800-90B Compliance | | |
| | NIST SP 800-90 A/B/C Compliance [in case of embedded DRBG] | | |
| | NIST SP800-22 Statistical Test Suite Compliance | | |
| | Die Harder Test suite Compliance | | |
| | ENT Test suite Compliance | | |
| Post-Processing | Post-Processing Algorithm used | | |
| Type of Interface | Entropy Output | | |
| | Management Interface | | |
| | Other Interfaces | | |
| Administration and Management | Command Line Interface (SSH) | | |
| | Built –in web server | | |
| | Syslog Alerting on GUI of remote monitoring system | | |
| | Secured User Access Management | | |
| Environmental | Operating temperature | | |
| | Storage temperature | | |
| | Humidity | | |

| | | | |
|---|---|---|---|
| | | Dimensions | |
| | Physical Characteristics | Weight | |
| | | Power Supply | |
| | Power Consumption | Power consumption (Normal operation) | |
| | | Power consumption (Idle Mode) | |
| | | Details of OS supported along with versions | |
| | OS supported | | |

| | | |
|---|---|---|
| | **CHAPTER-2** | |
| | **General Requirements** | |
| **2.1** | **Reference documents** | |
| 2.1.1 | Whatever that has not been specifically stated in this document, shall be deemed to be as per relevant latest ITU-T Recommendations and NIST SP 800-90 A/B/C standard. | This is the clause of GR for information purpose only |
| 2.1.2 | All references to TEC GRs & other Recommendations/standards imply their latest issues. | This is the clause of GR for information purpose only |
| **2.2** | **Engineering requirements** | |
| 2.2.1 | The manufacturer shall furnish the actual dimensions and weight of the equipment. | Architecture to be given by the |

| | | |
|---|---|---|
| | | manufacturer |
| 2.2.2 | The equipment shall be 19'' rack mountable. [Category A] | Physical Check |
| 2.2.3 | The equipment shall have a robust chassis, redundant power supplies and hot-swap redundant fans. [Category A] | Physical Check |
| 2.2.4 | It should be engineered to comply with environmental test requirements as defined in this document. | Declaration |
| 2.2.5 | The external plug-in units shall be of a suitable type to allow their removal/insertion while the equipment is in energized condition. [Category A/B/C] | Physical check |
| 2.2.6 | The mechanical design and construction of each card/unit shall be inherently robust and rigid under all conditions of operation, adjustment, replacement, storage and transport. | Physical check |
| 2.2.7 | Each sub-assembly shall be marked with schematic reference to show its function so that it is identifiable from the layout diagram in the handbook. | Physical check |
| 2.2.8 | Each terminal block and individual tags shall be numbered suitably with a clear identification code and shall correspond to the associated wiring drawings. [Category A/B/C] | Physical check |
| 2.2.9 | All external Interfaces / Controls / Indicators/Switches shall be clearly screen printed/marked on the unit to show their functional/connectivity diagrams and functions. [Category A & B] | Physical check |
| 2.2.10 | Important Do's and Don'ts about the operation of the system shall be indicated. [Category A & B] | Physical check |
| **2.3** | **Operational requirements** | |
| 2.3.1 | The equipment shall be designed for continuous operation and shall be tested for 72 hours of continuous working. | Covered in field trial. |
| 2.3.2 | The equipment shall be able to perform satisfactorily without any | Test certificate |

| | | |
|---|---|---|
| | degradation at an altitude up to 4000 meters above mean sea level. A test certificate from the manufacturer will be acceptable, in case no test facility is available. | from the manufacturer shall be submitted or Testing shall be carried out at an altitude up to 4000 meters above mean sea level |
| 2.3.3 | Visual indication to show power ON/OFF status shall be provided. | Physical check |
| 2.3.4 | QRNG shall be provided with software that includes drivers for the supported operating systems. | Manual Check |
| 2.3.5 | QRNG shall optionally provide a graphical interface to read and display random numbers and store them in a file. | Manual Check |
| 2.3.6 | Visual indications should be provided about the healthy and unhealthy conditions of the system. | Physical Check |
| **2.4** | **Quality requirements** | |
| 2.4.1 | The manufacturer shall furnish the MTBF value along with the methodology used for calculation. The minimum value of MTBF shall be 25,000 hrs. | Report/Declaration by the manufacturer to be submitted. |
| 2.4.2 | The equipment shall be manufactured in accordance with the international quality management system ISO 9001:2015 or latest issue. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted by the manufacturer. | Declaration/Certificate to be submitted for ISO 9001:2015 compliance. Quality plan describing the quality assurance system may be |

| | | |
|---|---|---|
| | | checked. |
| **2.5** | **Maintenance requirements** | |
| 2.5.1 | Maintenance philosophy is to replace faulty units/subsystems after quick online analysis through monitoring sockets, alarm indications and Built-in Test Equipment. [Category A/B/C] | Undertaking to be submitted by the manufacturer. |
| 2.5.2 | The equipment shall have easy access for servicing and maintenance. [Category A/B/C] | Physical check |
| 2.5.3 | The equipment shall have the provision to update the firmware. | Already Covered in Test Case No. 16 |
| 2.5.4 | Suitable alarms shall be provided for the identification of faults in the system and faulty units. The alarms may be placed on the QRNG Hardware and in the remote monitoring system. | Physical check |
| 2.5.5 | Ratings and types of fuses used are to be indicated by the supplier. | Physical check |
| **2.6** | **Power supply requirements for QKD Equipment** | |
| 2.6.1 | The equipment should work at a single phase AC mains supply of 230 V with variation in the range of +15% and -15% and frequency as 50 Hz +/-2Hz or uninterrupted –48V DC with a variation in the range from -40V to -60V. [Category A] | Declaration |
| 2.6.2 | The equipment shall operate over this range without any degradation in performance. | Declaration |
| 2.6.3 | The equipment shall be adequately protected in case of voltage variation beyond the range mentioned above and also against input reverse polarity in case of DC feeds. | Declaration |
| 2.6.4 | The derived DC voltages in the equipment shall have protection against over-voltage, short-circuit and overload. | Declaration |
| 2.6.5 | The equipment shall be power efficient. The actual power rating/ | Declaration |

| | | |
|---|---|---|
| | consumption is to be furnished by the manufacturer of the equipment | |
| 2.7 | **Accessories** | |
| 2.7.1 | The supplier shall provide a complete set of:<br>a) all the necessary connectors, connecting cables (including power cord) and accessories required for satisfactory and convenient operation of the equipment. Types of connectors, adapters to be used and accessories of the approved quality shall be indicated in the operating manuals.<br>b) Software, along with software version and the arrangement to load the software at site. | Check whether the complete details of the necessary connectors, connecting cables and accessories are required for satisfactory and convenient operation of the equipment are mentioned in the operating manual. |
| 2.7.2 | The source of the components/ accessories, from where these have been procured, is also to be submitted by the manufacturer. | The details to be submitted by the manufacturer. |
| 2.8 | **Documentation** | |
| | Technical literature in the English language only shall be accepted. All aspects shall be covered in the manuals. The manuals shall include the following: - | Check technical literature. |
| 2.8.1 | Installation, operation and maintenance manual<br>It should cover the following, as applicable to the category of the product:<br>(i) Safety measures to be observed in handling the equipment; | Check whether the Installation, operation and maintenance manual covers the required aspects. |

| | | |
|---|---|---|
| | (ii) Precautions for installation, operation and maintenance;<br>(iii) Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance, troubleshooting and sub-assembly replacement;<br>(iv) Illustration of internal and external mechanical parts. | |
| 2.8.2 | Repair Manual<br>It should cover the following:<br>i. List of replaceable parts used to include their sources and the approving authority.<br>ii. Detailed ordering information for all the replaceable parts shall be listed in the manual to facilitate the reordering of spares.<br>iii. Procedure for trouble-shooting and sub-assembly replacement shall be provided. Test fixtures and accessories required for repair shall also be indicated. A systematic troubleshooting chart (fault tree) shall be given for the probable faults with their remedial actions. | Check whether the Repair manual covers the required aspects. |
| **2.9** | **Operating personnel safety requirements** | |
| 2.9.1 | The Laser product, if used shall meet the Automatic Laser Shutdown (ALSD)/Automatic Power Reduction (APR) procedure of ITU-T Rec. G.664 (latest edition) on Class B laser. The equipment shall have visual warnings and controls ensuring danger-free operation. Laser safety signs and instructions must be mentioned in the equipment. | Physical check |
| 2.9.2 | Protection against short circuits/open circuits in the access points shall be provided. [Category A] | Physical check |
| 2.9.3 | The equipment shall have a terminal for grounding the rack. [Category A] | Physical check |
| 2.9.4 | All switches/controls on the front panel shall have suitable | Physical Check |

| | | |
|---|---|---|
| | safeguards against accidental operation. [Category A] | |
| 2.9.5 | The equipment shall be adequately covered to safeguard against entry of dust, insects, etc. [Category A/B] | Physical Check |
| **2.10** | **Environmental Testing Requirements** | |
| 2.10.1 | The instrument shall conform to the requirements for the applicable category as specified in TEC document TEC 14016:2010 {Old Document No: QM-333) {MARCH 2010 issue} "Standard for Environmental Testing of Telecommunication Equipment". | Report from TEC designated test lab to be submitted. |
| | | |
| | **Chapter 3** | |
| | **Safety & EMC requirements** | |
| **3.1** | **Safety Requirements [Category A/B/C]** | Report from TEC designated test lab to be submitted. |
| **3.2** | **Electromagnetic Interference** | Report from TEC designated test lab to be submitted. |
| **3.3** | **General Electromagnetic Compatibility (EMC) Requirements** | Report from TEC designated test lab to be submitted. |

# I. Detailed Test Cases

## Test Case No. 1

**Test Details:** Verification of high-level block diagram for the entropy source

**Clause No.: 1.6.2**

**Test Procedure:** Noise Source

**Step 1:** Enable “test mode”.

**Step 2:** Set the number of samples to be requested from the noise source.

**Step 3:** Request the samples from QRNG through the interface, eg. GetNoise (number_of_samples_requested).

**Step 4:** Capture the output:

i. noise_source_data: raw digitized samples

ii. status: TRUE/FALSE

**Expected Results:** Check if the status is TRUE and the number of samples matches the request.

**Test Procedure:** Conditioning Component / Post-processing

**Step 1:** Check if the QRNG includes a post-processing unit.

**Step 2:** If supported, note the details about its implementation (e.g., the hash function, cryptographic algorithms, and/or key size used).

**Step 3:** Check from the logs and/or GUI, the post-processing method selected and its parameters (e.g. key size, etc.) during initialization.

**Step 4:** Estimate the entropy as per the Test Case No. 16 for the raw data and also with the post-processing. Ensure output after post-processing maintains or enhances entropy and randomness.

**Step 5:** If the QRNG supports multiple post-processing algorithms, check the GUI-based selection or status display of post-processing options.

**Step 6:** Repeat Step 3 and Step 4 for all supported post-processing algorithms.

**Expected Results:** Ensure the output after post-processing maintains or enhances the entropy and randomness.

**Test Procedure:** Health Tests

**Step 1:** Note the details of various continuous and on-demand health tests supported by the QRNG, along with the conditions under which the health test fail.

**Step 2:** Check if the Repetition Count Test (RCT) and Adaptive Proportion Test (APT) is included in the continuous health tests. Monitor the output status of the continuous health tests.

**Step 3:** Choose type_of_test_requested (bitstring indicating test type or suite) e.g., 0001 = RCT, 0010 = APT, or manufacturer-defined code .

**Step 4:** Call HealthTest (type_of_test_requested).

**Step 5:** Capture the output status: TRUE (pass), FALSE (fail).

**Expected Results:**

i. Repetition Count Test (RCT) and Adaptive Proportion Test (APT) are supported as continuous health tests.
ii. Health Test runs and returns expected result.
iii. Failures are logged if the status is FALSE.
iv. Confirm fallback logic or blocking behavior if test fails.

## Test Case No. 2

**Test Details:** Verification of Entropy Assessment

**Clause No.** 1.6.10

**Test Procedure:**

**Step 1:** Enable the test mode.

**Step 2:** Fetch the raw data using CLI.

**Step 3:** Check the entropy value from GUI/CLI and it shall be atleast greater than the threshold specified by the manufacturer before post processing.

**Step 4:** In the case where no post processing component is used check that the entropy threshold specified by the manufacturer is as per clause 1.13.6

**Step 5:** Check whether an error status is generated in case the entropy of the raw data is below the specified threshold.

**Expected Results:** The entropy value should be greater than the threshold value specified by the manufacturer before post processing.

## Test Case No. 3

**Test Details:** Fetching Output of QRNG when post-processing component is not used

**Clause No.:** 1.7.5

**Test Procedure:**

**Step 1:** Use the CLI or GUI interface provided by the QRNG system to execute commands for data retrieval.

**Step 2:** Perform multiple operations changing the number of requested samples.

**Step 3:** Check metadata such as timestamps, data size, and source ID for each data fetch.

**Expected Results:** The QRNG system should consistently return random bit string without any errors.

## Test Case No. 4

**Test Details:** Fetching Output of QRNG when post-processing component is included

**Clause No.:** 1.7.6

**Test Procedure:**

**Step 1:** Use the CLI or GUI interface provided by the QRNG system to initiate a request for QRNG random data using the specified API or protocol. Ensure the system is in an operational state and post-processing is used. Check the status of the request message, if it is success.

**Step 2:** Enable the 'test' or ‘raw-access’ mode to access the quantum noise-source output.

**Step 3:** Execute the CLI or GUI interface as specified in the product documentation to collect raw data directly from the quantum noise source.

**Step 4:** Check metadata such as timestamps, data size, and source ID for the data fetches.

**Expected Results:** The QRNG system should consistently return random bit string without any errors using the post-processing component. The QRNG system shall return raw random bit string without any errors from the quantum noise-source output.

## Test Case No. 5

**Test Details:** Restriction to access raw quantum noise source samples under special circumstances

**Clause No.:** 1.7.7

**Test Procedure:**

**Step 1:** Create two users; User1 and User2, and assign user 1 the role to access the raw data.

**Step 2:** Enable the test mode and access the raw data using the user 1.

**Step 3:** Repeat step 2 for user 2.

**Expected Results:** The access to raw data should only be available to user 1.

## Test Case No. 6

**Test Details:** Behaviour of the Quantum Noise source

**Clause No.:** 1.8.2

**Test Procedure:**

**Step 1:** Enable the 'test' or ‘raw-access’ mode to access the quantum noise-source output. Obtain a sequential dataset of at least 100000 sample values obtained directly from the noise source.

**Step 2:** Plot the probability distribution of the collected sample values.

**Step 3:** Repeat Step 1 and Step 2 twice at different time intervals.

**Step 4:** Check the probability distributions of the Quantum noise source outputs do not change (within 1%)

**Expected Results:** Ensure that the probability distribution function of the Quantum noise source outputs do not change with time.

## Test Case No. 7

**Test Details:** Validation of Fixed-Length Output and output range from quantum noise source

**Clause No.:** 1.8.6

**Test Procedure:**

**Step 1:** Enable the test mode and access the bitstring outputs using the symbol size specified by the manufacturer. The output random bitstrings should match the symbol size.

**Step 2:** Enable the test mode and access the bitstring outputs using the symbol size less or more than that specified by the manufacturer. The output random bitstrings shall be either of the symbol size specified by the manufacturer or an error should occur.

**Step 3:** Disable the test mode and log the output bitstrings using CLI. From the logs ensure that the outputs are within the range as specified by the manufacturer.

**Expected Results:** All output bitstrings should match the specified fixed symbol size, and values fall within the documented output range specified by the manufacturer.

## Test Case No. 8

**Test Details:** Validation of additional noise source

**Clause No.:** 1.8.7 and 1.8.8

**Test Procedure:**

**Step 1:** Estimate the entropy of the additional noise source as per Test Case No. 16.

**Step 2:** Inject failure in the primary entropy source and request random numbers through interface.

**Expected Results:** The additional entropy source shall provide random bits in case of failure of primary noise source.

## Test Case No. 9

**Test Details:** Health Tests

**Clause No.:** 1.10.1

**Test Procedure:** Alarm for Health Tests

Simulate following failures in QRNG and observe alarm behaviour at the output for below mentioned failures and monitor the system via GUI/CLI and system logs for alarm notifications, error messages, or status flags.

(a) When the entropy reduces below the threshold.

(b) Failure of the Quantum Noise Source.

(c) Quantum Noise Source hardware failures

**Expected Results:** In each failure condition, check the QRNG system should detect the anomaly and raise a corresponding alarm or fault indication through logs, GUI alerts, or CLI status messages.

**Clause No.:** 1.10.2

**Test Procedure:** Health Tests

**Step 1:** Enable the test mode to access the quantum noise-source output.

**Step 2:** Check through the CLI system logs that the health status is available before post-processing.

**Expected Results:** The system should perform health tests before post-processing.

**Clause No.:** 1.10.3

**Test Procedure:** Startup health Tests (Power on Self Test)

**Step 1:** Power off the QRNG device completely and then power it on again to simulate a full system reboot.

**Step 2:** Observe the system's behaviour via the GUI and CLI interfaces immediately after reboot.

**Expected Results:** The system should automatically execute the startup health tests without manual intervention. The results of these tests should be clearly displayed in the system logs or GUI.

**Test Procedure:** Fault injection start up health test

**Step 1:** Inject a hardware fault like disconnecting or disabling the quantum noise source.

**Step 2:** Then perform a full system reboot by switching the QRNG power OFF and ON.

**Expected Results:** After reboot, the QRNG system should automatically run the startup health test. The test must detect the injected hardware failure and log appropriate error messages or raise alarms.

**Clause No.:** 1.10.4

**Test Procedure:** QRNG random data fetch during the Startup Health Tests

**Step 1:** Perform a full system reboot by powering off and on the QRNG.

**Step 2:** Immediately after the system restarts, attempt to collect QRNG random data using the CLI or GUI interface as per the specified protocol.

**Expected Results:** The QRNG should not provide any random data immediately after reboot. Any attempt to access data until the startup health test has been completed and passed; should return an error or a “not ready” status. Once the startup health test has passed, the QRNG should return a successful response along with random bit strings.. No errors or warnings should appear.

**Clause No.:** 1.10.14

**Test Procedure:**

**Step 1:** Power off the QRNG device completely and then power it on again to simulate a full system reboot.

**Step 2:** Note down the start-up tests run during the start-up. Check that the start-up tests includes the continuous health tests.

**Step 3:** Check through GUI or system logs that the start-up tests are run over atleast 1024 consecutive samples.

**Expected Results:** The start-up tests shall run on atleast 1024 consecutive samples.

## Test Case No. 10

**Test Details:** Continuous Health Tests

**Clause No.:** 1.10.5

**Test Procedure:**

Continuously monitor the QRNG system using either the GUI or by collecting system logs over a defined observation period (e.g., 30–60 minutes).Observe the health test entries generated during this period.

**Expected Results:** The GUI and logs must display periodic health test updates at regular intervals. These updates must include test results aligned with the NIST SP 800-90B standard, showing the status of entropy quality, test timestamps, and pass/fail indicators.

**Clause No.:** 1.10.6

**Test Procedure:**

Execute the QRNG CLI or GUI interface command to request random data

**Expected Results:** The response from the QRNG should include both the random data and a health status field indicating the operational condition of the quantum noise source and post-processing unit. The health status should confirm that the data is valid and was generated while the system was in a healthy state.

**Clause No.:** 1.10.8

**Test Procedure:** False positive probability

Monitor the QRNG system logs or GUI over a defined duration (e.g., 30–60 minutes).

**Expected Results:** The QRNG system must log or display continuous health test results at regular intervals. The false positive probability value shall be within the range of $2^{-20}$ to $2^{-40}$.

## Test Case No. 11

**Test Details:** On-Demand Health tests

**Clause No.:** 1.10.9

**Test Procedure:**

Continuously monitor the QRNG system using either the GUI or by collecting system logs over a defined observation period (e.g., 30–60 minutes).Observe the health test entries generated during this period.

**Expected Results:** The GUI and logs must display periodic health test updates at regular intervals. These updates must include test results aligned with the NIST SP 800-90B standard, showing the status of entropy quality, test timestamps, and pass/fail indicators.

**Clause No.:** 1.10.10

**Test Procedure:**

**Step 1:** Note down the types of on-demand health tests supported by the QRNG.

**Step 2:** Use the CLI or GUI to execute an on-demand health test by not restarting the entropy source. The CLI command shall specify the type or suite of tests to be performed.

**Expected Results:** The system must execute the health test successfully upon the command. Test results should be clearly displayed in both CLI and GUI interfaces, indicating if the entropy source passed the requested test.

**Clause No.:** 1.10.11

**Test Procedure:**

While an on-demand health test is running (via CLI or GUI), simultaneously execute the CLI or GUI interface to collect QRNG random data. Compare the data samples collected through the user interface with the samples internally used for the health test.

After the on-demand health test has fully completed (via CLI or GUI), compare the collected data behaviour with the product's documented handling policy for post-test samples.

**Expected Results:** The collected samples should not match those under test evaluation and the system must behave consistently with its defined policy—either allowing access to validated samples or discarding them. No errors should occur during data retrieval.

## Test Case No. 12

**Test Details:** Check disablement of bit stream in case of failure

**Clause No.:** 1.10.12

**Test Procedure:**

**Step 1** - Inject fault to fail the QRNG.

**Step 2**- Check if random bit stream from output of Quantum Entropy Source is disabled or not

**Step 3**- Check if normal operation is resumed after health test confirms normal state.

**Expected Results:** If a failure of the Quantum entropy source occurs while the QRNG is being operated, the random bit stream shall be disabled immediately, until an appropriate set of health tests confirm resumption of normal operational state of QES.

## Test Case No. 13

**Test Details:** Check disablement of bit stream in case of failure

**Clause No.:** 1.10.16

**Test Procedure:** Quantum Random Source Intermittent failures

Simulate an intermittent failure in the QRNG system—such as brief disruptions in the quantum noise source signal or momentary environmental anomalies. Monitor the QRNG system via CLI or GUI.

**Expected Results:** The system logs should indicate execution of continuous health tests. The health test results should clearly report the failure event and system response.

**Test Procedure:** Quantum Random Source Persistent failures

**Step 1:** Simulate a persistent hardware or system failure in the quantum noise source or related components (e.g., by disconnecting hardware or inducing constant signal failure).

**Step 2:** Observe the behaviour using the CLI and GUI interfaces.

**Step 3:** Attempt to execute the CLI interface to collect QRNG random data during the failure condition.

**Expected Results:** The CLI/GUI should clearly indicate a persistent failure state through logs, status messages, or alerts.

The system must return a fault response indicating that the entropy source has failed and is not providing valid output.

## Test Case No. 14

**Test Details:** Statistical Testing of Randomness

**Clause No.:** 1.12.1

**Test Procedure:** NIST SP 800-22 Test Suite

Run NIST SP 800-22 Test Suite on the output bits collected from the QRNG.

Get the executables for test suite from https://csrc.nist.gov/CSRC/media/Projects/Random-Bit-Generation/documents/sts-2_1_2.zip

And follow the steps mentioned in https://github.com/terrillmoore/NIST-Statistical-Test-Suite

**Expected Results:** Collected QRNG samples shall pass NIST SP 800-22 test suite.

**Test Procedure:** Dieharder Tests

Run Dieharder Tests on the output bits collected from the QRNG.

Follow the steps mentioned in the Robert G. Brown's General Tools Page

**Expected Results:** Collected QRNG sample shall pass Dieharder Test Suite.

**Test Procedure:** ENT Tests

Statistical Random Data test using ENT Tests.

Follow the steps mentioned in this link https://www.fourmilab.ch/random/

**Expected Results:** Collected QRNG sample shall pass ENT Test Suite.

## Test Case No. 15

**Test Details:** CHSH Bell Inequality Test

**Clause No.:** 1.12.2

**Test Procedure:** CHSH Bell Test

Calculate the CHSH inequality <S> if the QRNG uses entanglement,

Refer https://qubit.guide/6.3-chsh-inequality

QisKit Textbook: https://github.com/Qiskit/textbook/tree/main/notebooks/ch-demos#

**Expected Results:** Collected QRNG samples shall pass NIST SP 800-22 test suite.

## Test Case No. 16

**Test Details:** Min-Entropy Assessment

**Clause No.:** 1.13.2

**Test Procedure:**

**Step 1:** Collect data as per para 3.1.1 of NIST SP 800-90B.

**Step 2:** Check whether the entropy source is IID or Non-IID as per para 3.1.2 of NIST SP 800-90B.

**Step 3:** Estimate entropy as per Section 6.1 of NIST SP 800-90B in case of IID Track and Section 6.2 of NIST SP 800-90B in case of Non-IID Track

**Step 4:** Apply Restart Tests as per Section 3.1.4 of NIST SP 800-90B

**Step 5:** If the restart tests are passed, update the entropy estimate as per Section 3.1.4 of NIST SP 800-90B. If the restart tests is failed, the validation fails.

**Step 6:** Check whether the conditioning/post-processing is used or not.

**Step 7:** If the conditioning is used, update the entropy estimate as per section 3.1.5 of the NIST 800-90B.

**Step 8:** Check the min-entropy estimated is greater than 0.98.

**Expected Results:** The min-entropy estimated as per the Test procedure shall be greater than 0.98.

## Test Case No. 17

**Test Details:** Checking immediate detection of failure and detection of entropy degradation

**Clause No.:** 1.13.4

**Test Procedure:** Detecting Degree of Degradation

**Step 1:** Simulate a total system failure like complete shutdown of the quantum noise source or failure of internal hardware components.

**Step 2:** Make a request for fetching random numbers through the interface. The request response shall show ERROR status.

**Expected Results:** The response for the random number request shall show ERROR status in case of failure of noise source and entropy degradation.

## Test Case No. 18

**Test Details:** Alarm reporting

**Clause No.:** 1.13.5

**Test Procedure:**

Inject system failures and log the different types of alarms supported by the system:

| S.No. | Alarm Type | Description | Verify Alarm Generation |
|---|---|---|---|
| | *e.g. Failure of* | | |

| | | | |
|---|---|---|---|
| | *Noise Source, Entropy Degradation, etc.* | | |
| | | | |

**Expected Results:** Check whether system generates and logs alarms in case of failures

## Test Case No. 19

**Test Details:** Checking the stability of QRNG by changing date and time

**Clause No.:** 1.13.7

**Test Procedure:**

**Step 1-** Power on the QRNG and check normal operation

**Step 2-** Change the system date and time or generate events such as changeover of millennium/century, leap year etc.

**Step 3-** Verify changes through timestamps in the logs.

**Step 4-** Fetch random numbers through the interface.

**Expected Results:** Check normal working of QRNG hardware and software.

## Test Case No. 20

**Test Details:** Secure update of firmware

**Clause No.:** 1.13.8

**Test Procedure:**

**Step 1:** Check Existence of Firmware Update Mechanism

Verify if the QRNG has:

i. Bootloader or secure update module

ii. Defined method for firmware ingestion (e.g., via USB or secure web

interface)

**Step 2:** Test Secure Update with Authenticated Image - Prepare a signed firmware image (using manufacturer's signing key) and upload the firmware via the supported interface.
Verify: The device accepts the update. Reboots correctly and loads the new firmware. Logs (if any) show authentication and success.

**Step 3:** Test Rejection of Unauthenticated Image
Modify the firmware binary or corrupt the signature or use an unsigned or tampered image.
Observe: Rejection of the update and No installation or boot from the corrupted image and Logs indicating failure reason. In case of failure, the device shall rollback to original firmware/backup/recovery state firmware as designed by manufacturer.

**Step 4:** Test Rollback/Downgrade Protection (if applicable). Load an older, valid signed image. Try to downgrade. Observe whether the device accepts or rejects firmware rollback and log the attempt.

**Expected Results:**

i. Check whether Device supports a documented update process.
ii. Check logs for authentication success and failure and record observations.
iii. Check that Device prevents or logs firmware rollback attempts unless done by admin.

## Test Case No. 21

**Test Details:** Checking simultaneous multiple requests from applications

**Clause No.:** 1.13.9

**Test Procedure:**

Step 1: Connect and initialize the QRNG device.

Step 2: Prepare a script for the multiple requests from applications

Step 3: Collect and store output for each request in separate files.

Step 4: Monitor for errors, delays, crashes, or dropped requests.

**Expected Results:** Verify that all requests are successful.

## Test Case No. 22

**Test Details:** Checking if QRNG is capable of operating in more than one mode

**Clause No.:** 1.13.11

**Test Procedure:**

Request for operating mode of QRNG through API

**Expected Results:** QRNG should return information about the mode in which it is operating, upon request.

## Test Case No. 23

**Test Details:** QRNG supplies random numbers through a secure standard interface and provide protection against unauthorized access

**Clause No.:** 1.13.12

**Test Procedure:**

**Step 1:** Verify documentation for the QRNG's supported standard interfaces (e.g., USB-HID, PCIe, REST API, etc.).

**Step 2:** Check if communication is encrypted (e.g., TLS for APIs, secure protocol for drivers or any other protocol defined by manufacturer).

**Step 3:** Install and initialize QRNG on the host system.

**Step 4:** Attempt to access the QRNG from an unauthenticated or unauthorized application.

**Step 5:** Verify that access is denied and logged appropriately.

**Step 6:** Run a legitimate client/application that is authenticated via API key, certificate, token, or user identity.

**Step 7:** Request random numbers from the authorized client and verify successful access.

**Step 8:** Test multiple sessions with different identities (authorized and unauthorized).

**Step 9:** Inspect logs for proper authentication, access control events, and error messages.

**Step 10:** Optionally, Attempt privilege escalation or bypass methods to access the random data without authentication and verify interface resilience against tampering or replay of previously authenticated sessions.

**Expected Results:** Verify the access logs and record observations accordingly. Confirm compliance with interface and access control standards (e.g., FIPS, ISO/IEC 19790).

## Test Case No. 24

**Test Details:** Input Request Format

**Clause No.:** 1.13.14

**Test Procedure:**

Step 1: Initiate a request for random bits by specifying the following parameters:

- size: Number of random bits requested
- source: the source of the random bits (processed or raw)
- format (optional): binary, hex, JSON, etc.

Step 2: Vary the size of the random bits requested and observe the output.

Step 3: Obtain the output in different formats (a) Binary (b) Hex and (c) JSON.

**Expected Results:** The system shall support the specified parameters.

## Test Case No. 25

**Test Details:** Output Data Format

**Clause No.:** 1.13.15

**Test Procedure:**

Initiate a request for random bits and check through CLI the following parameters are mentioned in the output response::

- unique ID of the Quantum Entropy Source
- random bytes (encoded in base64 for JSON format)
- mode (raw or processed random numbers)
- timestamp
- status (True if the request has been satisfied, otherwise false)
- health status

**Expected Results:** The specified parameters shall be available in the output response.

## Test Case No. 26

**Test Details:** Generation of system logs for audit

**Clause No.:** 1.13.17

**Test Procedure:**

**Step 1:** Enable System logging

**Step 2:** Capture system logs for a defined period of 30-45 minutes.

**Step 3:** Generate all type of logs like Request, Response, warning, Information, Error, Debug, etc. as per manufacturer documentation.

**Expected Results:** Verify correctness of logging levels and generation of logs as per respective system event.

## Test Case No. 27

**Test Details:** Online Performance Monitoring

**Clause No.:** 1.13.20

**Test Procedure:**

**Step 1:** Power On and Initialize the QRNG

**Step 2:** Check the following information are accessible on the GUI:

(a) Entropy of the Output

(b) Status of Health Tests

(c) Other performance parameters, if any

**Expected Results:** The performance parameters shall be displayed properly on GUI.

## Test Case No. 28

**Test Details:** QRNG Physical Security Testing

**Clause No.:** 1.14.7

**Test Procedure:**

**Step 1:** Initiate physical intrusion to the device.

**Step 2:** Check system behaviour after tamper simulation and observe whether tamper detection triggers alarms.

**Step 3:** Attempt CLI access using a wrong password

**Step 4:** Review internal logs or audit trails to confirm all unauthorized access attempts are recorded.

**Expected Results:** Unauthorized access is blocked and alarms are recorded.

## J. Summary of Test Results

TEC Standard No._____

TEC Test Guide No._____

Equipment name & Model No._____

| *Clause No.* | *Compliance* (Complied /Not Complied / Submitted/Not Submitted / Not Applicable) | *Remarks / Test Report Annexure No.* |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

*[Add as per requirement]*

*Date:*

*Place:*

*Signature & Name of TEC testing Officer /*

** Signature of Applicant / Authorized Signatory*

** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatory shall be the same as the one for Form 'A'.*

----End of the document----