

PUBLIC

Rules and Procedures for IoT System Certification Scheme

(STQC/IoTSCS/D01)

Issue: 1.0



IoT System Certification Scheme

STQC Certification Body

STQC Directorate,

MeitY, Government of India

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 2 of 25

Contents

0.1 Approval and Issue.....	4
0.2 Amendment Record.....	5
1.0 Introduction	6
2.0 Objective	6
3.0 Purpose	7
4.0 Scope and overview of Certification	7
4.1 IoT System Scope	7
4.2 Assessment Level	8
4.3 IoT devices scheme assessment methodology	8
4.4 Assessment Process Flow.....	9
4.5 Web Application Security as per OWASP ASVS	13
4.6 Mobile Application Security as per OWASP MASVS	13
4.7 Vulnerability Assessment/Penetration Testing (VA/PT) as per CIS Benchmark	13
4.8 Security Architecture/Design Review	13
4.9 Code Review.....	14
5.0 References	14
6.0 Definitions:.....	14
6.1 Certification Agreement.....	17
6.2 Certification Body	17
6.3 Legal Status	17
6.4 Roles and functions of Certification Body.....	17
7.0 Organization description.....	18
7.1 Organization Structure and top Management.....	18
7.2 List of Appointments	19
8. Records.....	19

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 3 of 25

9. Documents and Change Control	19
10. Confidentiality.....	20
11. Liability.....	20
12. Appeals, Complaints and Disputes.....	20
13. Changes in the Certification Requirements	21
14. Certification Procedure	21
14.1 Registering for Certification	21
14.2 Scope Identification	21
14.3 Application review	21
14.4 Nomination of Testing/Evaluation Lab	21
14.5 ComplianceAssessment	22
14.6 Completion of Testing/Evaluation	23
14.7 Certification.....	24
15. Suspension and Withdrawal/Cancellation of Certification.....	24
15.1 Suspension	24
15.2 Withdrawal/Cancellation	24
16. Disclaimer.....	25
17. Indemnity:.....	25

 गुणोत्कर्षे समृद्धिः	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
	Page : 4 of 25	

0.1 Approval and Issue

This document is the property of IoT System Certification Scheme under the ambit of STQC Certification Body (SCB) and should not be reproduced in part or full without the written consent.

Reviewed by : Management Representative

Approved by : Head, IoTSCS Scheme

Note:

- Management Representative is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 6 of 25

1.0 Introduction

The digital space has witnessed major transformations in the last couple of years and as per industry experts would continue to evolve itself. The latest entrant to the digital space is the Internet of Things (IoT). IoT can also be defined as interplay for software, telecom and electronic hardware industry and promises to offer tremendous opportunities for many industries.

With the advent of the Internet of Things (IoT), fed by sensors soon to number in the trillions, working with intelligent systems in the billions, and involving millions of applications, the Internet of Things will drive new consumer and business behavior that will demand increasingly intelligent industry solutions, which, in turn, will create enormous opportunity for IT industry and even more for the companies that take advantage of the IoT.

The launch of the Digital India Program of the Government, which aims at ‘transforming India into digital empowered society and knowledge economy, will provide the required impetus for development of the IoT industry in the country. The various initiatives proposed to be taken under the Smart City concept and the Digital India Program to setup Digital Infrastructure in the country would help boost the IoT industry.

Internet of Things (IoT) refers to a vast network that provides an interconnection between various objects and intelligent devices. The three important components of IoT are sensing, processing, and transmission of data. Nowadays, the new IoT technology is used in many different sectors, including the domestic, healthcare, telecommunications, environment, industry, construction, water management, and energy. IoT technology, involving the usage of embedded devices, differs from computers, laptops, and mobile devices. Due to exchanging personal data generated by sensors and the possibility of combining both real and virtual worlds, security is becoming crucial for IoT system. Furthermore, IoT requires lightweight encryption techniques. The goal of this scheme is to verify and validate the security mechanisms implemented in device and IoT eco System with their level of effectiveness.

2.0 Objective

IoT has three main pillars that are data collection, data transmission, and data security. To collect data, many sensing tools have been introduced and adapted to the IoT devices. For transferring collected data, various protocols have been developed and adapted in order to enable to the IoT devices to connect to existed networks and exchange data. Consequently, many classic and recent security issues are closely related to the IoT as well as authentication, data security, authorization, etc. Indeed, a weakness in authentication can lead to numerous attacks, including replay attack, Mirai attack, Denning–Sacco attack, denial of service attack, password guessing attack, etc.

The objective of this scheme is to promote security of IoT ecosystem. This scheme will facilitate improvement of National Cyber Security profile.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 7 of 25

The implementation of this Certification Program is to provide confidence to users that the risks associated with the threats currently set forth in the IoTSCS are addressed by a device/system provider through conformance to this scheme. Demonstration of conformance through this certification program provides formal recognition of a conformance to the industry standards.

3.0 Purpose

This document is intended to be used primarily by Applicant (Manufacturer, Integrator, Supplier, and User etc.), the Certification Body, and evaluation/testing labs. This document describes the organization of Certification Body and processes of certification, which by means of testing/evaluation of IoT system and devices are conforming to the specified requirements of the applicable standard, procedures.

4.0 Scope and overview of Certification

At present, all the IoT products/system are covered under this scheme. The Scheme scope may be categories as below: -

4.1 IoT System Scope

Evaluation of IoT system covers assessment of all the Sensing and embedding components (includes Sensors, Actuators etc), communication protocols, IoT Gateways, IoT cloud, End-user devices and user interface etc. Following activities are in scope of testing based on the system.

- IoT Devices Security as per ISO/IEC 27402 IoT security and privacy — Device baseline requirements and verification requirement – ‘OWASP ASVS Appendix C: Internet of Things Verification Requirements’
- Security Architecture and Design Review as per best practices and code analysis as per OWASP
- IoT System Security as per ‘ISO/IEC 27400 Cybersecurity — IoT security and privacy — Guidelines’ which includes the following other standards/ methodology
 - Web Application Security as per OWASP ASVS
 - Mobile Application Security as per OWASP MASVS
 - API Security as per OWASP API Top 10
 - Vulnerability Assessment/Penetration Testing (VA/PT) as per CIS Benchmark/ Best Practices
 - Security Architecture/Design Review as per best practices

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 8 of 25

- Code Review as per OWASP
- Risk Analysis Report

4.2 Assessment Level

Level of Assessment is defined for IoT devices only which will be used in IoT system. Assessment of IoT devices covers basically three aspects mainly software, firmware, hardware and its application interfaces. Assessment covers testing of IoT devices conducted by using both invasive and non-invasive attack methodology. The IoT devices scheme comprises of three (03) levels, with each higher level being more comprehensive in the assessment. There are 3 different level of assessment, covering different security requirements. The objective of testing under each of the levels are summarized in IoT device scheme assessment Levels below:

Assessment Level	Description	Applicable Standards
1	IoTVS Level 1 requirements aim to provide a security baseline for connected devices which does not allow an attacker to move laterally to other devices or systems on the IoT ecosystem.	Requirements mentioned in ISO/IEC 27402 IoT security and privacy — Device baseline requirements and Level 1 of OWASP ASVS Appendix C: Internet of Things
2	IoTVS Level 2 is for IoT devices that contain sensitive data, which requires protection and is the recommended level for most devices.	Requirements mentioned in ISO/IEC 27402 IoT security and privacy — Device baseline requirements and Level 2 of OWASP ASVS Appendix C: Internet of Things
3	IoTVS Level 3 is for the most critical IoT devices that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.	Requirements mentioned in ISO/IEC 27402 IoT security and privacy — Device baseline requirements and Level 3 of OWASP ASVS Appendix C: Internet of Things

4.3 IoT devices scheme assessment methodology

The IoT devices assessment scheme comprises three (03) levels, with each higher level being more comprehensive in the assessment. The detailed requirements of testing under each of the levels are given in document STQC/IoT/F04:Checklist for Auditors/Assessors. The assessment methodology is summarized below:

Assessment Level	High level Assessment Requirements	Description
------------------	------------------------------------	-------------

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 9 of 25

1	Security Baseline Requirements IoTVS Level 1 requirements aim to provide a security baseline for connected devices which does not allow an attacker to move laterally to other devices or systems on the IoT ecosystem.	Developer/ sponsor is required to provide compliance to checklist (level 1) with suitable evidences. Developer/ sponsor submit the test report along with testing methodology, evidences, and sample product.
2	Security Medium Requirements IoTVS Level 2 is for IoT devices that contain sensitive data, which requires protection and is the recommended level for most devices.	Developer/ sponsor is required to provide compliance to checklist (level 2) with suitable evidences. Developer/ sponsor submit the test report along with testing methodology, evidences, and sample product.
3	Critical Requirements IoTVS Level 3 is for the most critical IoT devices that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.	Developer/ sponsor is required to provide compliance to checklist (level 3) with suitable evidences. Developer/ sponsor submit the test report along with testing methodology, evidences, and sample product.

4.4

a. Assessment Process Flow for IoT Devices

1. Developer/ sponsor contact the certification body along with application form, product operational manual, design document, deployment /environment document, internal test report, test methodology, evidences, sample product and requisite fee for registration.
2. CB will review the application and finalize assessment level. CB appoints the Assessor and Testing Laboratory.
3. Testing laboratory will test and review the claimed compliance by the vendor against checkpoints.
4. Testing laboratory submit the test report along with testing methodology and evidences for evaluation to Assessor.
5. The Assessor submits the evaluation report to CB.
6. CB organizes certification committee (CC) meeting. CB issues certificate of compliance to developer based on CC recommendation and product is listed on STQC website.

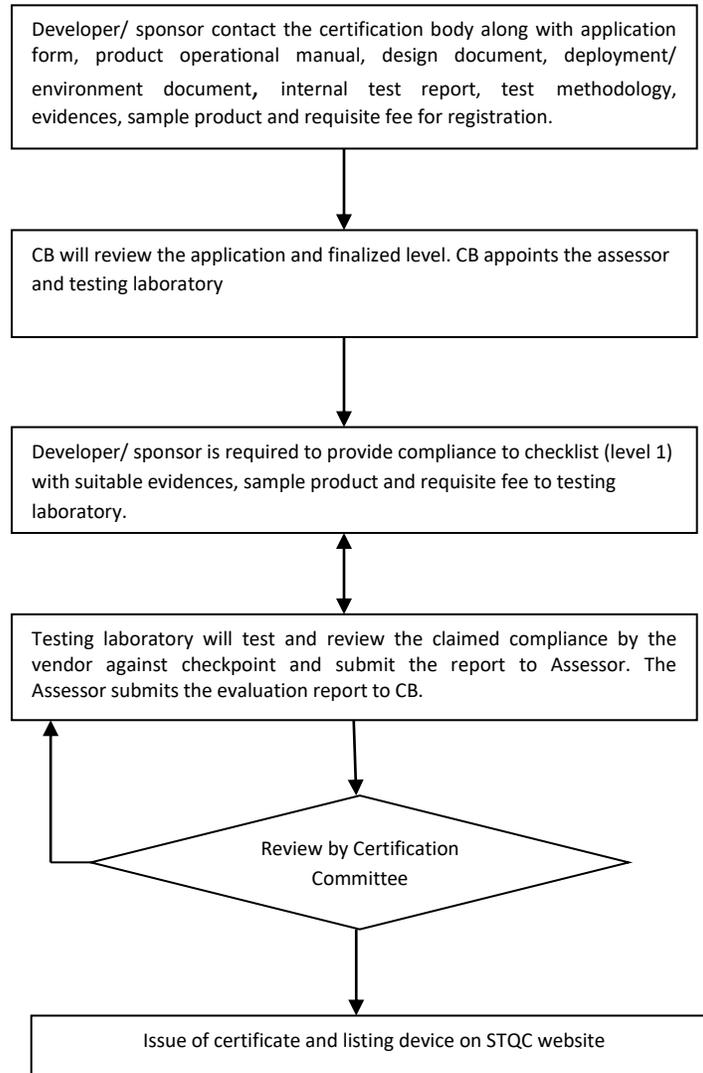
	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 10 of 25

b. Assessment Process Flow for IoT System

1. Developer/ sponsor contact the certification body along with application form, system operational manual, design document for software and IoT devices, deployment/ environment document, Risk Analysis Report for IoT System and requisite fee for registration.
2. CB will review the application for completeness. CB appoints the Assessor and Testing Laboratory.
3. Developer/ sponsor is required to provide compliance to IoT system checklist along with suitable evidences. Developer/ sponsor also submit the following reports as mentioned below:
 - a. Details of Identified risks along with applicable controls for IoT system
 - b. Test Report related to devices as per Clause 4.3
4. Testing laboratory will review/test the claimed compliance by the vendor against checkpoints wherever required and submits the following test reports to Assessor.
 - a. Test Report related to all software & host system used in IoT system (Web Application Security as per OWASP ASVS, Mobile Application Security as per OWASP MASVS, API Security as per OWASP and Vulnerability Assessment/Penetration Testing (VA/PT) as per CIS Benchmark/ best practices)
5. The Assessor submits the evaluation report to CB.
6. CB organizes certification committee (CC) meeting. CB issues certificate of compliance to developer based on CC recommendation and system is listed on STQC website.

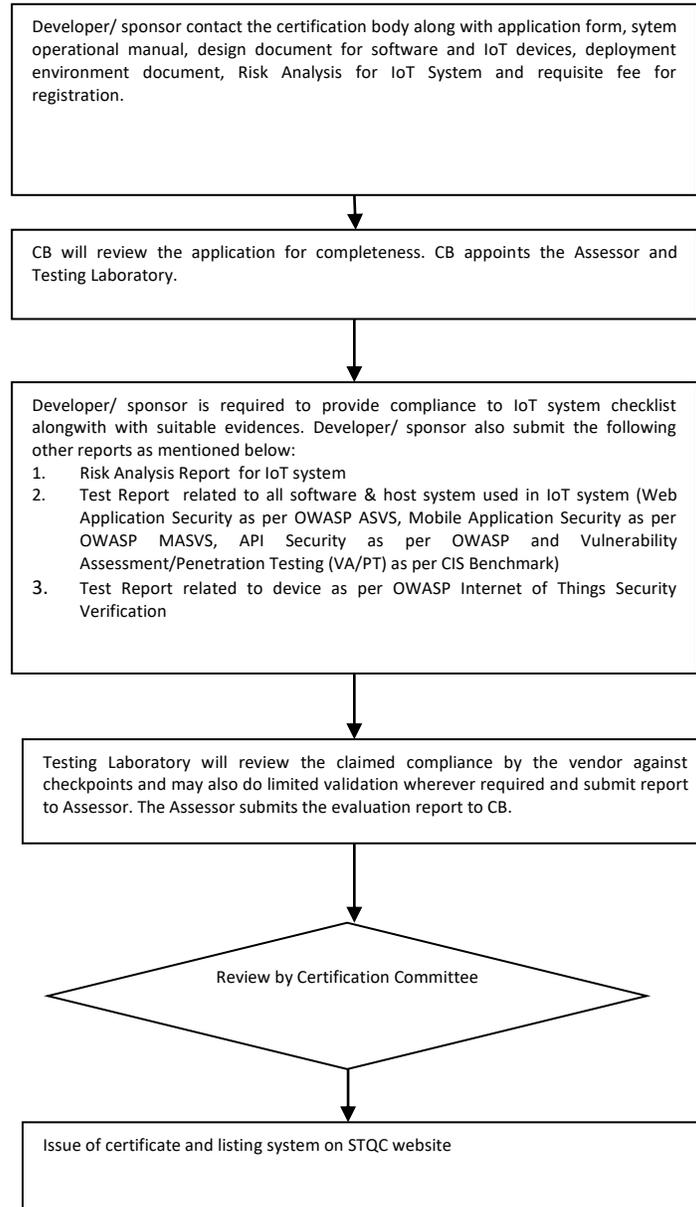
	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 11 of 25

Assessment Process Flow for IoT Devices



	IoT System Certification Scheme (IoTSCS)	Issue : 1.0
	Rules and Procedures (STQC/IoTSCS/D01)	Issue Date: 15-12-2023
		Page : 12 of 25

Assessment Process Flow for IoT System



	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 13 of 25

4.5 Web Application Security as per OWASP ASVS

Web application security include processes, technologies, or methods for protecting web servers, web applications, and web services such as APIs from attack. Application security will be assessed based on latest OWASP guidelines.

4.6 Mobile Application Security as per OWASP MASVS

Mobile application security refers to secure mobile applications from adversary. App security will be assessed based on OWASP MASVS. The MASVS defines two security verification levels (MASVS-L1 and MASVS-L2), as well as a set of reverse engineering resiliency requirements (MASVS-R). MASVS-L1 contains generic security requirements that are recommended for all mobile apps, while MASVS-L2 should be applied to apps handling highly sensitive data. MASVS-R covers additional protective controls that can be applied if preventing client-side threats is a design goal.

4.7 Vulnerability Assessment/Penetration Testing (VA/PT) as per CIS Benchmark Best practices

A vulnerability assessment is the process of identifying security issues and assign severity levels to as many security defects as possible in a given timeframe. Penetration testing is a process of identify breakpoint and holes in security posture of system. Both processes involved both automated and manual techniques. VA activity will be based on CIS or other similar benchmarks.

4.8 Security Architecture/Design Review

The objective of this activity is for the developer to provide a description of the security architecture and design of the product. This will allow analysis of the information that, when coupled with the other evidence, will confirm the product achieves the desired properties. The security architecture and design descriptions support the implicit claim that security analysis of the product can be achieved by examining the product.

Security Architecture is a mechanism for protecting the security function in a product and ensures their proper behavior even when the security function themselves become target of an attack. A security architecture is a set of properties that the security function exhibits; these properties include self-protection, domain separation, and non-bypassability.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 14 of 25

The goal of design documentation is to provide sufficient information to determine the security function boundary, and to describe how the security function implements the security requirements.

4.9 Code Review

Code review is systematic examination of computer source code and reviews are done in various forms and can be accomplished in various stages. A security review of the IoT product may uncover common security bugs as well as the issues specific to business logic of the application. The checklist should cover the most critical security controls and vulnerability areas such as: Data Validation, Authentication, Session Management, Authorization, Cryptography, Error Handling, Logging, Security Configuration and Network Architecture.

5.0 References

STQC/IT&eGov/D00	Quality Manual
STQC/IT&eGov/D01	Schedule of Charges
STQC/IT&eGov/F02	Agreement with applicant for certificate of approval
STQC/IT&eGov/F01	Master List of documents
OWASP ISVS	OWASP Internet of Things Security Verification Standard (ISVS)
ETSI EN 303 645	Cyber Security for Consumer Internet of Things: Baseline Requirements
ISO/IEC 27400	Cybersecurity — IoT security and privacy — Guidelines
ISO/IEC 27402	ISO/IEC 27402 IoT security and privacy — Device baseline requirements
OWASP ASVS	OWASP Application Security Verification Standard (ASVS)
No.26(1)/2019-IPHW	National Electronics Policy, 2019

6.0 Definitions:

For the purpose of this document, the following definitions, shall apply.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 15 of 25

- **administrator:** user who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality
- **associated services:** digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality.
- **authentication mechanism:** method used to prove the authenticity of an entity
- **authentication value:** individual value of an attribute used by an authentication mechanism
- **best practice cryptography:** cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques
- **constrained device:** device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use
- **consumer:** natural person who is acting for purposes that are outside her/his trade, business, craft or profession
- **consumer IoT device:** network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables
- **debug interface:** physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functionality
- **device manufacturer:** entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers
- **factory default:** state of the device after factory reset or after final production/assembly
- **initialization:** process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access
- **initialized state:** state of the device after initialization
- **IoT product:** consumer IoT device and its associated services

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 16 of 25

- **isolable:** able to be removed from the network it is connected to, where any functionality loss caused is related only to that connectivity and not to its main function; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured
- **logical interface:** software implementation that utilizes a network interface to communicate over the network via channels or ports
- **manufacturer:** relevant economic operator in the supply chain (including the device manufacturer)
- **network interface:** physical interface that can be used to access the functionality of consumer IoT via a network
- **owner:** user who owns or who purchased the device
- **personal data:** any information relating to an identified or identifiable natural person
- **physical interface:** physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer
- **public security parameter:** security related public information whose modification can compromise the security of a security module
- **remotely accessible:** intended to be accessible from outside the local network
 - **security module:** set of hardware, software, and/or firmware that implements security functions
- **security update:** software update that addresses security vulnerabilities either discovered by or reported to the manufacturer
- **sensitive security parameters:** critical security parameters and public security parameters
- **software service:** software component of a device that is used to support functionality
- **telemetry:** data from a device that can provide information to help the manufacturer identify issues or information related to device usage
- **unique per device:** unique for each individual device of a given product class or type
- **user:** natural person or organization.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 17 of 25

6.1 Certification Agreement

An agreement which is part of the Certification System and which details the mutual rights and obligations of the certificate holder and the Certification Body, and which includes the right to use the certificate, Ref STQC/IT&eGov/F02.

6.2 Certification Body

This body conducts certification for compliance/conformity with respect to published standards and any supplementary documentation required under the system.

All the operations and functions of the Certification body will be performed by STQC Directorate as per Quality Manual, STQC/IT&eGov/D00.

6.3 Legal Status

Ref Section 2.1 of STQC/IT&eGov/D00 (Quality Manual)

6.4 Roles and functions of Certification Body

All the procedures adopted by the Certification Body are administered in a non-discriminatory manner. The Certification Body makes its services accessible to all eligible applicants, without any undue financial or other conditions.

The Certification Body under Labeling of IoT System Certification Scheme:-

- Confines its assessment and decision on certification to those matters specifically related to the scope of certification being considered.
- Has a defined scope determination criterion against which the Devices/Processes of an applicant is assessed. In case of change in specification for any process/design/requirement viz-a-viz certification criteria, the acquirer has to undergo for fresh certification.
- Is responsible for its decision relating to the granting, maintaining, extending, reducing, suspending and withdrawing certifications.
- Has an identified management structure, which has the overall responsibility for the operation of Certification System.
- Has a documented structure, including provisions to assure the impartiality of the operation of Certification Body.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 18 of 25

- Has a documented system to provide confidence in its ability to operate a certification system.
- Ensures that each decision on certification is taken by persons different from those who carried out the testing/assessment/evaluation/audits.
- Has defined authorities and responsibilities relevant to its certification activities.
- Has adequate arrangements to cover liabilities arising from its operations and/or activities. (as specified in certification agreement).
- Has financial stability and resources required for the operation of the certification system, in the form of budgetary and resource support from STQC Directorate. The financial administration of the scheme including determination of charges is the responsibility of Head (Certification Body).
- Has sufficient number of personnel having the necessary education, training, technical knowledge and experience for performing certification functions under the overall responsibility of Head (Certification Body).
- The Certification Body's personnel along with Head (Certification Body) are free from any commercial, financial and other pressures, which might influence the results of Certification process.
- Has a defined criterion for appointment and operation of all the committees needed for Certification process. These committees are free from any commercial, financial and other pressures that might influence decisions.
- Has a defined policy and procedure for resolution of Complaints, Appeals and Disputes received from suppliers or other parties about the handling of certification or any other related matter.

Note: Refer Quality manual for further details.

7.0 Organization description

7.1 Organization Structure and top Management

The STQC Certifications Body for Labeling of Consumer and industrial IoT system Certification Scheme are as follows:-

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 19 of 25

- A Chairman
- An Advisory Board
- Management Committee
- Certification Committee
- SCB's Personnel
- Head Operations Personnel/scheme representative(s)

Refer Quality Manual (STQC/IT&eGov/D00), Cl. 3.1 for Composition, Term of References and business proceedings.

7.2 List of Appointments

Refer document, STQC/IT&eGov/D04 – “List of Appointments” identifies the personnel & other resources involved in the activities of STQC Certification Body for this scheme.

The responsibilities of all personnel involved in the certification activities are indicated in the document, STQC/IT&eGov/D06– “Responsibility Matrix”.

8. Records

The Certification Body maintains a record system to comply with existing procedures. The records demonstrate that the certification procedures have been effectively implemented, particularly with respect to application forms, audit reports, test reports and other documents relating to granting, maintaining, extending, reducing, suspending or withdrawing certification. The records are identified, managed and disposed of in such a way as to ensure the integrity of the process and confidentiality of the information. These records are kept for at least one full certification cycle (i.e. 3 Years).

9. Documents and Change Control

Certification body maintains a formal document control system where all procedures, specifications etc. are controlled by Doc. No., Version No., and Records/ History of amendments and approval of changes. A master list of approved documents indicating above is maintained by certification body.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 20 of 25

Refer Procedure for Document Control (STQC/ IT&eGov /P01) and Record Control (STQC/ IT&eGov/P02)

10. Confidentiality

The Certification Body has adequate arrangements, consistent with applicable laws, to safeguard confidentiality of the information obtained in the course of its certification activities at all levels of its organization, including committees and external bodies or individuals acting on its behalf.

The information obtained for the certification purposes shall not be disclosed to a third party without the written consent of the supplier. Where the law requires information to be disclosed to a third party, the supplier will be informed of the information provided as permitted by the law.

Ref Clause 2.5 of Quality Manual (STQC/IT&eGov/D00)

11. Liability

The Certificate of Compliance given to applicant, here in referred to as “Acquirer”, under the scheme shall not be regarded as in any way diminishing the mutual contractual responsibilities/obligations between the supplier and purchaser. While the Certificate of Compliance will normally be a sound indicator of the capability of supplier to provide quality products/applications/ services, it should not be taken as a sort of guarantee accorded by the Certification Body. The Certification Body will not be liable for any deficiency in the products/service supplied by supplier. Ref Document for Approval / Certification Agreement (STQC/IT&eGov/D03).

12. Appeals, Complaints and Disputes

Appeals, Complaints and Disputes brought before the Certification Body by suppliers or other parties are subject to the review of Technical Advisory Committee.

The Certification Body

- Keeps records of all appeals, complaints and disputes and remedial actions relative to certification
- Take appropriate corrective and preventive action
- Document the actions taken and assess their effectiveness.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 21 of 25

Refer Procedure for Appeal Procedure (STQC/IT&eGov/P01) and Complaint Procedure (STQC/IT&eGov/P02)

13. Changes in the Certification Requirements

The STQC Certification Body will give due notice of any changes it intends to make in its requirements for certification under IoTSCS. The decision of STQC Directorate on the grounds of National Cyber Security will be final and the outcome will be conveyed to the interested parties.

14. Certification Procedure

14.1 Registering for Certification

The applicant shall submit duly filled prescribed application form (Ref STQC/IoTSFS/F01) along with following documents to the certification body and requisite fee in advance as per quotation received from STQC Labs:

- Certification Agreement
- Scope identification
- Bharat Kosh Payment Receipt & Service Request Form of STQC Lab
- Filled Response for compliance against checklist

Valid **Digitally Signed** Soft Copy Documents as mentioned above shall be acceptable.

14.2 Scope Identification

The Organization discusses the scope of assessment to the satisfaction of the Certification Body. The objective of this activity is to identify the assessment level of a IoT system

14.3 Application review

The Certification Body shall scrutinize the completeness of application with relevant documents.

14.4 Nomination of Testing/Evaluation Lab

Certification Body shall nominate Testing/Evaluation Lab for carrying out the testing/Evaluation as per the prescribed checklist. The size of the auditing shall be decided on the basis of the finalized scope. Ref Quality Manual (STQC/IT&eGov/D00).

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 22 of 25

14.5 Compliance Assessment

The scopes of assessment shall be finalized and application shall be submitted by the applicant organization along with all process and implementation evidences which will be reviewed by the assessment team. The observation or any discrepancy may be clarified with the applicant before proceeding for assessment.

The Testing/Evaluation Lab will make the testing/evaluation plan and share the same with organization and Certification Body.

14.6 Guidance for Evaluation methodology for product series

This methodology allows developers and sponsors to evaluate the security of their products. In this context, some developers or sponsors might need to evaluate a Product series instead of a single product.

Input Required:

- **Differential Analysis Report (DAR)**

In order to distinguish between different products within a Product series, the developer must produce a document called Differential Analysis Report (DAR). This document identifies the shared features, and differences, between the considered products and how these differences may affect to the security objectives. Refer F02 document for further guidance for content of DAR.

- **Selection of the Reference IoT Product**

The developer must select, within the Product series, a Reference IoT Product. If no single IoT Product is representative of the whole series, the developer should either chose several Reference IoT Products in order to cover the whole series, or restrict the scope of the series.

- **Testing Reuse Rationale (TRR)**

The developer must produce a rationale describing its strategy for reusing test results of the Reference IoT Product(s), based upon the DAR. This Testing Reuse Rationale (TRR) justifies how a sample of tests can be executed on a sample of products, in order to ascertain the security behavior of all the products within the Product series declared in the

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 23 of 25

applicable Security Target. This document also contains the rationale for the selection of the Reference IoT Product(s).

- **Deliverables**

The developer must provide the whole Product series, i.e. the Reference IoT Product and the Other declared products. At any moment during the evaluation, the Testing lab may require the access to any product belonging to the series. The Testing lab independently decides on which product(s) they want to execute a given test, and justifies their choice in the ETR.

Note:

- The Certification Body/Validator may challenge the selection of Reference IoT Product(s) at any moment during the evaluation, and may require additional workload to be allocated, in order to perform further tests on the product series. In that case, the sponsor may restrict the scope of the evaluation to the Reference IoT Product(s) only.
- The evaluator shall perform dedicated tests on the other declared products if the DAR or the results in the evaluation activities suggests a possible difference in behavior between different products
- In case of multiple variants of same SoC and /or Firmware, the evaluation facility should provide the suitable evidences.

14.7 Completion of Testing/Evaluation

Once the Testing/Evaluation lab has completed the Testing Report/Checklist (Ref Form No. STQC/IoTSCS/F04) against the proposed scope of certification, report will be submitted Certification Body and remains with the Certification Body. The Certification Body reviews the submitted documents and for consistency and completeness and to determine whether:

- The Certification Evidences and other relevant documents are complete.
- The Testing/Evaluation Report is unambiguous.

If the Certification Body believes the Testing/Evaluation lab findings are insufficient, then the Certification Body may require the testing/evaluation lab to provide clarification or additional rationale to support the findings.

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 24 of 25

14.8 Certification

Certification Committee evaluates compliances in holistic way and integrates information from all channels stated above. Based on compliances submitted by Certification Body along with Certification Committee recommendation, certificate of approval is issued to applicant. The validity of the “Certificate of Approval” will be issued for three years from date of issue subjected to successful demonstration during surveillance audit. The Certificate shall be issued in three labels for IoT devices.

The Certification body has all rights to publish the name of certification applicant and scope of certification in STQC website.

15. Suspension and Withdrawal/Cancellation of Certification

15.1 Suspension

Certification may be suspended for a limited period, at the discretion of Certification Body under the following circumstances:

- Continuous complaints from users.
- If the certified supplier is not regularly involved in the activities for which he is certified.
- If there has been any other contravention of the applicable requirements or rules of procedures of certification body.
- Fail to provide conformance during surveillance audit
- In interest of National Security, if product is found to be having adverse effect to National Cyberspace and users

The official communication by the Certification Body of the suspension will be either through a registered letter or equivalent means. The Certification Body will publish notification of the withdrawal/cancellation.

15.2 Withdrawal/Cancellation

The Certification Body will cancel certification; withdraw the Certificate under the following circumstances

- If the product/service under suspension fails to rectify non-conformance within specified period (Six months)
- If the product/service provider (organization) either will not or cannot ensure conformance to changed rules of procedure of Certification Body
- In interest of National Security, if product is found to be having adverse effect to National Cyberspace and users

	IoT System Certification Scheme (IoTSCS)	
	Rules and Procedures (STQC/IoTSCS/D01)	Issue : 1.0
		Issue Date: 15-12-2023
		Page : 25 of 25

- If the product/service developer ceases to maintain the applications

The official communication by the Certification Body of the withdrawal/cancellation will be either through a registered letter or equivalent means. The Certification Body will publish notification of the withdrawal/cancellation.

16. Disclaimer

- The auditing & certification services and the results there of are provided on this scheme basis without warranty of any kind. STQC disclaim any and all warranties, express or implied, including without limitation any warranties of merchantability or fitness for a particular purpose with respect to the audited services and the audit results.
- In no event shall STQC or any of their respective officers, directors, subsidiaries, parents or affiliates be liable to anyone claiming through applicant, for any special, indirect, incidental or consequential damages of any kind or for any damages whatsoever resulting from reliance on the audit results.
- If the Labeling of Consumer and industrial IoT system Certification Scheme applicant passes the audits/tests as per requirements, Scheme provider will be entitled to disclose the fact that the processes passed the audit to third parties. Notwithstanding the foregoing, all right, title and interest in and to the audit results, including without limitation, the copyright thereof, remains with STQC.

17. Indemnity:

The applicants will indemnify STQC against any misuse of STQC Name and Logo. For any misuse of STQC name and logo, the supplier themselves will be held responsible. STQC will take necessary actions for such cases. STQC will not be responsible for any miscommunication or harm caused to any party because of any misrepresentation of its name and logo by the intermediary or any other interested party.

The empanelled suppliers will not use the Name of STQC and its Logo, to promote their interest in any manner in any programme not connected / related or being undertaken for STQC.

Ref Documents STQC/IT&eGov/D02.