IoT System Certification Scheme



P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01
Date : 21-05-2024
Page : 1 of 34

Procedure for CCTV Testing Evaluation and Certification (STQC/IoTSCS/P01)

Issue: 01



IoT System Certification Scheme (IoTSCS) STQC Directorate, Ministry of Electronics & Information Technology (MeitY) Government of India

IoT System Certification Scheme



P01 — Procedure for CCTV Testing Evaluation and Certification

Issue :	01
Date :	21-05-2024
Page :	2 of 34

Contents

0.1.	Approval and Issue	3
0.2.	Amendment Record	4
1.	Background	5
2.	Purpose	5
3.	Objective	5
4.	Reference Documents	5
5.	Principal and Approach	5
6.	Procedure	.7
7.	1. The certification of the CCTV Cameras:	.7
7.	2. Steps for CCTV Cameras Certification Process	.7
7.	Certificate	8
Ann	exure-A TCF requirements for CCTV Cameras	9

Public IoT System Certification Scheme IoT System Certification Scheme Issue : 01 Date : 21-05-2024 Page : 3 of 34

0.1.Approval and Issue

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

Reviewed by : Management Representative

Approved by : Head, IoTSCS

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



P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024 Page : 4 of 34

0.2.Amendment Record

Sl. No.	Date	Issue	Rev.	Reason of Change /Change Details
1.	May 2024	1	0	First Issue

IoT System Certification Scheme



P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024 Page : 5 of 34

1. Background

IoT System Certification Scheme (IoTSCS) is operated by STQC Directorate, Ministry of Electronics and Information Technology (MeitY), Govt. of India. Under supervision of CB, the Testing Laboratories perform Testing of CCTV Cameras against the Essential Requirements mentioned in Gazette Notification dated 6 Match, 2024 issued by MeitY.

2. Purpose

The purpose of this document is to define the methodology to verify the compliance of claims made by CCTV developer/manufacturer with respect to Essential Requirements mentioned in Gazette Notification dated 6 Match, 2024 issued by MeitY.

3. Objective

The key objective is that the CCTV Cameras shall comply with the requirements as specified in the Essential Requirements mentioned in Gazette Notification dated 6 Match, 2024 issued by MeitY.

CCTV developer/manufacturer vendor may implement TEE on Single chip (i.e. Micro Controller, Micro Chip, Secure Processor, Secure Chip etc.) or set of chips on single PCB.

4. Reference Documents

STQC/IoTSCS/D01 :		Rules and Procedures
REGD. No. D. L3300	4/99	: Gazette Notifications dated 6^{th} March, 2024 issued by MeitY
ISO 27001 :		Information Security Management System
ISO/IEC 17065 :		Conformity assessment Requirements for bodies Certifying
		products, processes and services
ISO/IEC 17025 :		General Requirements for the Competence of Testing and
		Calibration Laboratories.

(Please refer Master List of Documents for latest version of the documents)

5. Principal and Approach

To build confidence on the security of the CCTVs, the overall approach is based on following principles. Since in this type of product, different functions of device manufacturing are performed by expert agencies or specialist contractors as part of supply chain, necessitating designing **assurance methodology** based on following principles:

STCC ।। गुणोत्कर्धे समृधिः ।।।

IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024 Page : 6 of 34

- Use of principles of secure product design
 - Identify the problem context by defining security objectives and identifying security requirements in the context of CCTV cameras
 - Perform Threat modelling to identify countermeasures for secure system design
 - $\circ\,$ Incorporate System security engineering processes (NIST SP 800-160) as solution context
- Use of Principles of demonstrating system trustworthiness: by combination of assurance mechanism and compliances. This is a decision-making context that provides an evidence-based demonstration, through reasoning, that the system–of-interest is deemed trustworthy based upon a set of claims indicating achievement of security objectives. The trustworthiness context consists of:
 - Developing and maintaining the assurance case for fulfilment of claims to prove its truthiness and
 - Demonstrating that the assurance case is satisfied. This can be done with the combination of the following techniques:
 - "Statement of compliance and/or declarations" of CCTV Developer/Manufacturer as per Essential Requirements mentioned in Gazette Notification dated 6 Match, 2024 issued by MeitY.

Note: The person who signs the declaration should be associated legally with the company (i.e. Director) and should have DIN number (Director Unique Id Number issued by MCA).

- Verification of artefacts, demonstrating compliance obtained through certification/compliance programmes.
- Demonstration of compliance by CCTV Cameras Manufacturer/Developer using their procedures as test script, test jigs and other necessary tools and instrumentation which are validated.
- Validations by STQC test labs or STQC recognized expert agencies.
 - CCTV Developer/Manufacturer should provide production sample and/or an Engineering model with access probes to facilitate compliance testing.
 - CCTV Developer/Manufacturer should provide necessary Tools, Development Kit/Engineering Board with access probes to facilitate compliance testing.

IoT System Certification Scheme



P01 — Procedure for CCTV Testing
Evaluation and Certification

Issue :	01
Date :	21-05-2024
Page :	7 of 34

The CCTV Developer/Manufacturer shall prepare "System Security Engineering Manual" (or Technical Construction File (TCF)) which focuses on implementation mechanisms. The TCF shall define and establish problem, solution and trustworthiness contexts to ensure the security of a system, which is based on achieving a sufficiently complete understanding of the problem as defined by a set of stakeholder security objectives, security concerns, protection needs, and security requirements. This shall be evaluated using the artifacts requested in the Essential Requirements.

6. Procedure

7.1. The certification of the CCTV Cameras:

The CCTV Developer/Manufacturer shall identify the entities in its supply chain for design manufacturing, quality assurance and supply of chips through an entity relationship diagram highlighting the role and relationship and details of various critical entities. The number of entities could be different for different technical architectures and business models. In some cases, these entities are different specialist contractors or expert agencies and in other cases, a single agency may perform all the operations. Broadly, these specialist contractors cover different entities of the life cycle stages of concept, design & development, production, utilization, support, retirement.

The security controls exercise by CCTV Developer/Manufacturer should be as per Essential Requirements – Technical specification. Detail artefacts, demonstrating compliance, declarations etc. shall be submitted to STQC in the form of Technical Construction File (TCF).

7.2. Steps for CCTV Cameras Certification Process

- 1 CCTV Developer/Manufacturer to study Gazette Notification dated 6 Match, 2024 issued by MeitY to meets the requirements of Essential Requirements (Annexure A).
- 2 CCTV Developer/Manufacturer should prepare a detailed technical solution architecture demonstrating capability of CCTV Camera with Essential Requirements mentioned in Notification dated 6 Match, 2024 issued by MeitY.
- 3 Certification Body will evaluate document submitted and if found prima facie worthy of the proposed TCF, may schedule detailed technical review with presentation and discussion to explain architecture and its merit.
- 4 The CCTV Developer/Manufacturer should prepare themselves by developing secure-boot code, secure-update support, crypto library, test cases and required artifacts as defined in the Annexure A. Ensure to follow a secure engineering process to create the CCTV Camera.
- 5 CCTV Developer/Manufacturer shall prepare device design guidelines/instructions and provide necessary tools to be used by the device provider and this list should be part of

IoT System Certification Scheme



TCF. (like tool to load device Firmware, IDE, guidelines to use Tamper protection etc)

- 6 CCTV Developer/Manufacturer applies to STQC for CCTV certification by submitting application and technical construction file (TCF). The contents of technical construction file should at least consists of
 - a) The artifacts defined in the Essential Requirements
 - b) Artifacts to be used for test cases for verification and validation purpose. (Engineering board, demo board etc)
- 7 CB may allocate the application number under the scheme and same will be communicated to Test Laboratory.
 - a) Based on application number, CCTV Developer/Manufacturer shall contact Test Laboratory for proposal, SRF, submission of charges and test samples.
 - b) Test laboratory shall evaluate the CCTV Cameras based on TCF submitted, Vendor shall provide necessary support as and when required by Test Laboratory.
 - c) CCTV Developer/Manufacturer should demonstrate testing and validation as defined under the demonstration section of the Essential Requirements.
 - d) Laboratory will submit the final test report including TCF review report to CB
 - e) Laboratory will also submit final TCF (if any change) for the TCF submitted by CCTV Developer/Manufacturer as per Essential Requirements.
- 8 The Certification body will appoint Assessor for this evaluation. They will be continuously associated with this evaluation on behalf of Certification body to oversee the evaluation including witness testing, review of observation report and preparation of Test Report etc.

7. Certificate

Certification committee evaluates compliances in holistic way and integrates information from all channels stated above. Based on compliances along with Certification Committee recommendation, certificate of approval is issued to CCTV Developer/Manufacturer.

The validity of the certificate will be issued for three years from date of issue subjected to surveillance audit.

IoT System Certification Scheme



P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024 Page : 9 of 34

Annexure-A TCF requirements for CCTV Cameras

Technical Construction File (TCF) submitted by CCTV developer/manufacturer to IoTSCS Certification Body shall document: -

• Compliance/demonstration/validation to ALL applicable clauses as per Essential Requirements

mentioned in Notification dated 6 Match, 2024 issued by MeitY.

To create confidence on CCTVs, Manufacture shall maintain Technical Construction File having following information. Vendor need a provide information pertaining to the entire requirements mentioned below. **General**

<u>ucneru</u>								
Sl.No	Requirements from Vendor	Details need to be provided						
1.	General description of IoT Device, usage of IoT device and environment of use.							

<u>Certificates</u>

Sl.No	Requirements from Vendor	Details need to be provided
1.	Certificate for ISO 9001 (Scope should cover IoT Device Development, Manufacturing and Service (Manufacturer).	
2.	Certificate for ISO 9001 (Scope should cover IoT Device Supply of IoT Device (Supplier/ Distributor) if applicable.	
3.	Certificate of Incorporation (Manufacturer).	
4.	Certificate of Incorporation (Supplier).	
5.	Manufacturer authorization to supplier to place devices in Indian Market if applicable.	

Securing a CCTV (Closed-Circuit Television) system is crucial to protect sensitive information and ensure the system operates effectively. Key areas of testing include exposed network services, device communication protocols, physical access to the device's UART, JTAG, SWD, etc., the ability to extract memory and firmware, firmware update process security and storage and encryption of data. Here are brief requirements for the security of a CCTV system:

- 1. Physical Security Use tamper-resistant camera enclosures and locking mechanisms to deter physical tampering.
- 2. Access Control by Authentication, Role-Based Access Control (RBAC) and regularly review and update access permissions to reflect personnel changes.
- 3. Network Security by employing encryption of data transmission
- 4. Software Security by Regular Updates, Disable Unused Features and Strong Password Policies

IoT System Certification Scheme



P01 — Procedure for CCTV Testing Evaluation and Certification

Issue	:	01
Date	:	21-05-2024
Page	:	10 of 34

5. Penetration Testing: Employ penetration testing to assess the system's resistance to cyberattacks and address vulnerabilities.

The validity of the "Certificate of Approval" will be issued for three years from date of issue. **Essential Security Requirements**

Sr. No.	Category	Testing Parameter	What to be tested	Documents Required	Implement ation Details	Comm ent by Develo
					Detuns	per Yes/N
1.	Hardware Level Security Parameter (supported by software)	1.1 Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.	 Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation Testing, in presence of OEM team, to verify the enabling/disablin g of all the ports 	The vendor shall provide the following: a. Datasheet of the SoC being used in the device. b. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. c. Process flow of the Manufacturing/ Provisioning of the device		

					Publ	ic		
STOC	IoT S	IoT System Certification Scheme						
	D01 Drogodur	1 — Procedure for CCTV Testing aluation and Certification			Issue : 01			
गुणोत्कर्धे समृध्दि :	Evaluation and C				Date : 21-05-2024			
				Page :	11 of 34			
		and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware-based debuggers and access control mechanisms in case the interface is enabled. 4. Process audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning. [For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub						
	1.2 Verify that cryptograp hic keys	components/peri pherals.] Identifying all the keys and certificates being used in the device	Vendor submit following:	shall the				
	and	eco-system and	1. List of al	l keys				



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 12 of 34

	certificates	verification	and certificates	
	are unique	through:	being used in the	
	to each	 Testing, in 	device ecosystem	
	individual	presence		
	device.	of OEM	2. Key management	
		team	life cycle (purpose,	
		• Code	generation,	
		review	storage,	
		Process	destruction/zeroiz	
		audit of	ation, validity, key	
		the key-	changeover/rotatio	
		life cycle	n)	
		process		
	1.3 Verify	1. Identification	The vendor shall	
	that on-chip	of the availability	provide the	
	debugging	of debugging	following:	
	interfaces	interfaces such as		
	such as	USB, UART, and	a. Datasheet of the	
	JTAG or	other serial	SoC being used in	
	SWD are	variants	the device.	
	disabled or	through the	_	
	that	Datasheet of the	b. Documentation	
	available	SoC being used in	related to	
	protection	the device under	ports/interfaces	
	mechanism	test	enabled in the	
	is enabled		production devices	
	and	2. Verification	and the related	
	configured	and validation of	access control	
	appropriate	tne // / / / / / / / / / / / / / / / / / /	mechanism for	
	ıy.	ports/interfaces	protection of the	
		enabled in the	same.	
		production	a Dracaca flare of	
		uevices and the	the	
		related access	ule Manufacturing /Dro	
		control mochanism for	Manufacturing/P10	
		nrotoction of the	dovico	
		same as declared	uevice	
		in the vendor		
		documentation		
		3. Testing in		
		presence of OEM		
		team, to verify the		
		,, i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.		



IoT System Certification Scheme

Public

STOC		1				
				Issue :	01	
।। गणोत्कर्धे सम्रधिः :।।	गुणोत्कर्षे समृद्धिः ।।		ıg	Date :	21-05-2024	
Inguiss signan				Page :	13 of 34	
				- 0-		
		enabling/disablin g of all the ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware based debuggers and access control mechanisms in case the interface is enabled. 4. Process audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning. [For instance, through Block connections between the host microcontroller and its		Page :		
		interactions with various sub				
		components/peri				
	1.4 Verify	Identifving	The vendo	or shall		
	that trusted	whether	provide	the		
	execution is	TEE/SE/TPM is	following:			



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 14 of 34

			1
implemente d and enabled, if available on the device SoC or CPU.	available or not in the device through the SoC datasheet and technical documentation submitted by the vendor.	 Datasheet of the SoC being used in the device. User manual/ Technical specifications of the device 	
	Further assessment is done on the basis of scenarios as applicable to device as defined below:	3. Code snippets of the TEE API call, wherever applicable	
	CASE1:TEE/SE/TPMisnot available:		
	CASE 2: TEE/SE/TPM is available and enabled: Verification through code- review that crypto functions are called through TEE/SE/TPM APIs.		
	CASE 3: TEE/SE/TPM is available but not enabled by the vendor: Termed as non- conformance to the requirement.		



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 15 of 34

	OEM is required		
	to enable and		
	TEE/SE/TPM.		
1.5 Ver	ify Identifying all the	Vendor shall	
that	keys and	submit the	
sensitive	certificates being	following:	
data,	used in the device	1 List of all large	
private	eco-system,	1. LIST OF all Keys	
certificate	their storage	heing used in the	
are stor	ed mechanism(s).	device ecosystem	
securely	in and verification	device ceosystem	
a Secu	ire through:	2. List of all the	
Element,	• Testing, in	sensitive data with	
TPM, T	EE presence	their intended	
(Trusted	of OEM	usage and secure	
Execution	team	storage	
Environm	e • Code	mechanism(s) as	
nt),	or review	implemented along	
protected	Process	with secure	
using	audit of	be enabled in the	
cryptogra	n life cycle	device	
hv.	p nrocess	uevice.	
	process	3. Key management	
		life cycle (purpose,	
		generation,	
		storage,	
		destruction/zeroiz	
		ation, validity, key	
		changeover/rotatio	
		n) private keys and	
		certificates.	
1.6Verify	Testing, in	Vendor shall	
the	presence of OEM	submit the	
presence	of team, to verify the	following:	
tamper	measures		
resistance	e implemented in	1. Measures	
and/or	the device to	available in the	
tamper	prevent software	device to prevent	
detection	and hardware	software	



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 16 of 34

	features.	tampering.	tampering.	
			2. Measures	
			available in the	
			device to prevent	
			hardware	
			tampering.	
	1.7 Verify	Testing, in	Vendor shall	
	that any	presence of OEM	submit the	
	available	team, to verify the	following:	
	Intellectual	enabling of the		
	Property	Intellectual	1. Datasneet of the	
	protection	Property	50L	
	technologie	protection	2 Degumentation	
	s provided	novidad by the	2. Documentation	
	by the chip	chin	Intellectual	
	ar are	manufacturer if	Property	
	enabled	available	nrotection	
	enablea.	available.	technologies	
			provided by the	
			chip manufacturer	
			which have been	
			enabled.	
			3. In case, no	
			Intellectual	
			Property	
			protection	
			technologies are	
			being provided by	
			the chip	
			manufacturer, then	
			a declaration	
			stating the same.	
	1.8 Verify	Testing, in	Vendor shall	
	the device	presence of OEM	submit the	
	validates	team, to verify the	tollowing:	
	the boot	tollowing:		
	ımage		1. Datasheet of the	
	signature	1. Device boots	SoC	
	before	up successfully	0	
	loading.	with the	2. Technical	
		aocumented	specifications of	



Public IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 17 of 34

	 secure boot process when a valid boot image is provided. 2. Device does not boot up when a tampered boot image (like with missing signature, invalid signature) is provided. 	the device regarding secure boot (should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.)	
1.9 Verify usage of cryptograp hically secure pseudo- random number generator on embedded device (e.g., using chip- provided random number generators)	Verification of the documentation provided by the vendor regarding the random number generators being used in the device. Verification through code- review that random number generators or related libraries as applicable are being used in the device.	Vendor shall submit the documentation regarding the random generators (either hardware based or software based or both) being used in the device with their intended usage. In case, hardware based random number generators are being used, vendors shall submit the following: 1. Datasheet of the SoC 2. Technical specifications of the device regarding random generators	



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024 Page : 18 of 34

2.	Software/Fir	2.1 Verify	Testing, in	In case, software based random number generators are being used, vendors shall provide the libraries being used for the same. Vendor shall	
	mware	that memory protection controls such as ASLR and DEP are enabled by the embedded/ IoT operating system, if applicable.	presence of OEM team, to verify the declared memory protection controls available and enabled in the device using command line based tools/commands or any other open source tool like DEP, EMET tool.	submit the declaration of the memory protection controls available and enabled in the device.	
		2.2 Verify that the firmware apps protect data-in- transit using transport layer security.	 Verifying that strong encryption algorithms and secure TLS version is supported by the device to establish secure communication. Verifying that device properly validates the server's TLS certificate to ensure that it is trusted and has not been tampered with. Testing for 	The vendor shall submit the specifications and documentation related to the configurations available in the applications and firmware related to transport layer security.	

				Public
STOC	IoT	cification Sc	heme	
	P01 — Procedur	e for CCTV Testi	Issue :	01
गुणोत्कर्धे समृध्दिः	Evaluation and (Certification	Date :	21-05-2024
			Page :	19 of 34
		 vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites. 4. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval. 5. Verifying that theTLS session(s) are resistant to attemptsof interception and decryption of network traffic using man-in-the- middle attacks using tools like Burpsuite. 		
	2.3 Verify that the firmware apps validate the digital signature of server connections	1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following: 	Vendor mentioning the use-cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital	



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 20 of 34

	related to	signatures of the	
	secure	server connections.	
	server		
	connectio		
	ns and		
	digital		
	signaturo		
	validation		
	implemen		
	tod liko		
	strong		
	cinher		
	suites		
	Sacura		
	TIS		
	version		
	SCI SIGIL		
	ninning		
	etc		
	supported		
	by code		
	walkthrou		
	σh		
	g		
	Proper		
	• Troper		
	validation		
	Valluation		
	, cortificato		
	chain		
	validation		
	and		
	cortificato		
	revocatio		
	n chacks		
	II CHECKS		
	imnlomen		
	tod in the		
	device		
	uevice.		
	2 Testing for		
	2. resume 101		
	which can affect		
	which can anect		

Г	[Publ	ic
STOC	IoT S	System Cert	ificatio	on Scl	neme	
	P01 — Procedure for CCTV Testing		Issue : 01			
।। गुणात्कध समृध्धः ।।	Evaluation and C	Certification		Date :	21-05-2024	
				Page :	21 01 34	
		the security of TLS connection such as padding oracle attacks, or weak cipher suites. 3. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval. 4. Verifying that TLS session(s) are resistant to attemptsof interception and decryption of network traffic using man-in-the- middle attacks using tools like Burnsuite				
	2.4 Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.	Securecodereview[bothautomatedandmanual],inpresence of OEMteam,usingalicensedstaticanalysistoolthroughanyofthefollowingapproaches:1.Visittotheevaluationagencybythevendor	Vendor provide : 1. Fi binaries fo review. 2. Interna review repo	shall rmware or code al code orts		



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 22 of 34

with the	
Concernent of the second secon	
firmware code	
and installing the	
licensed static	
analysis tool	
analysis tool	
available with the	
evaluation agency	
in their systems.	
[Recommended]	
2 Visit to the	
2. VISIT to the	
evaluation agency	
by the vendor	
with the	
firmware code	
and any licensed	
and any incensed	
static analysis	
tool available	
with them and	
demonstrating	
the code review	
activity in the	
activity in the	
presence of	
representatives	
of evaluation	
agency.	
2 Civing a remote	
5. diving a remote	
access of the	
systems at	
vendor site to the	
evaluation agency	
for installing their	
licongod static	
analysis tool	
available with	
them.	
4. Giving a remote	
access of the	
systems at	
vendor site to the	
evaluation agency	
containing the	

Public



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 23 of 34

	firmware code		
	along with the		
	licensed static		
	analysis tool		
	available with the		
	vendors.		
2.5 Verify	Verification of the	Vendor shall	
that each	submitted list of	submit the	
firmware	third party	following:	
maintains a	components by	0	
software	running	1. Documentation	
bill of	automated tools	for information on	
materials	like FACT on the	software bill of	
cataloging	firmware.	materials,	
third party		including third-	
component	Identifying	party components	
S,	vulnerabilities in	and versions.	
versioning,	the third party		
and	component(s)	2. Organization	
published	through	process and	
vulnerabilit	publically	policies for the	
ies.	available	following:	
	vulnerability		
	databases	Addressing	
		and	
	Verification and	patching	
	validation of the	any	
	process defined	identified	
	by the vendor for	vuinerabilit	
	providing regular	les in third-	
	and natchos for	party	
	the firmware to	component	
	address any	5.	
	known	Informing	
	vulnerabilities in	the	
	third-narty	customore	
	components	about the	
	p	security	
		issues or	
		vulnerabilit	
		ies and	
		providing	
		security	



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 24 of 34

		updates and patches for the same. 3. Configuration management system and related policies for maintaining firmware and third party binaries, libraries and frameworks along with the patches/fixes issued to the devices.	
2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	Independent secure code review [both automated and manual] using a licensed static analysis tool through any of the following approaches: 1. Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] 2. Visit to the	 Vendor shall provide : Firmware Firmware binaries for code review. Internal code review reports 	

				Public		
STOC	IoT System Certification Scheme					
	D01 Date		Issue :	01		
गूणोत्कर्धे समुध्दि :	Full — Procedure	e for CCTV Testil Vertification	Date :	21-05-2024		
2			Page :	25 of 34		
	Γ	1				
		evaluation agency by the vendor with the firmware code 				
		analysis tool				
		available with the				
		vendors.	Vandara -1 11			
	2.7 Verify	1. Identifying the	vendor shall			
	firmware	the device	mentioning the			
	apps pin	establishes the	use-cases when the			
	the digital	server	device establishes			



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 26 of 34

	signature to	connections with	server connections	
	a trusted	the external	with the external	
	server(s).	world and	world, with	
		verifying the	detailed	
		following:	information about	
		ronormgi	the security	
		 Socurity 	mansuras in place	
		• Security	while welideting	
		leatures,	while valuating	
		related to	the digital	
		secure	signatures of the	
		server	server connections.	
		connectio		
		ns and		
		digital		
		signature		
		validation		
		as		
		implemen		
		ted like		
		strong		
		cinher		
		suites		
		secure		
		TIS		
		I LJ		
		33L ninning		
		pinning		
		etc.		
		supported		
		by code		
		walkthrou		
		gh.		
		 Proper 		
		certificate		
		validation		
		,		
		certificate		
		chain		
		validation		
		and		
		certificate		
		revocatio		
		n checks		
		aro		
		alt		1



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 27 of 34

2.8VerifyTesting,inVendorshsecuritypresence of OEMsubmittcontrols areteam, to verify thedocumentationin place tosecurity controlsregardingthinderasprovided bysecurity controlsfirmwarethevendortoplacetohinderreversehinderfirmwareengineeringreverseengineering.(e.g.removaengineering.engineering.lof verboseengineering.debuggingsymbols).submitt2.9VerifyTesting,inVendorthatthepresence of OEMsubmittfirmwareteam, to verify themeasuresimplemented in tupdatemeasuresimplemented in tdevice to makenotthedevice toresistant to tim	implemen ted in the device.	
2.9 Verify Testing, in Vendor sh that the presence of OEM submit t firmware team, to verify the measures update measures implemented in t process is implemented in device to make not the device to resistant to tim	2.8Verify presence of OEM presence of OEM submitVendor shall submitsecurity controls are in place to hinderpresence of OEM team, to verify the security controls regarding the security controls place to hinder firmware reverse engineering l of verbose debugging symbols).Vendor mesting, 	
to time-of- to time-of-use time-of-use attacks.	2.9 Verify Testing, in Vendor shall that the presence of OEM submit the firmware team, to verify the measures update measures implemented in the process is implemented in device to make it not the device to resistant to time- vulnerable make it resistant of-check vs. time- to time-of- to time-of-check of-use attacks.	
2.10Verify the device uses signing and validates firmware upgradeTesting, presence of OEM team, to verify the of achieving secu- firmware upgra which shou consist of ke involved and the management l documented process when a validation proce and any oth secure mechanism if implemented.Vendor shou submit the proce of achieving secu- firmware upgra which shou consist of ke involved and the management l documented 	2.10Verify the device uses signing and validates firmware upgradeTesting, presence of OEM team, to verify the following:Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure upgrade process when a valid updateVendor shall submit the process of achieving secure firmware upgrade involved and their management life cycle*, signature secure upgrade if implemented.2. Device does not2. Device does not	



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 28 of 34

	tampered update package (like with missing signature, invalid signature) is provided.		
2.11 Verify that the device cannot be downgrade d to old versions (anti- rollback) of valid firmware.	Testing, in presence of OEM team, to verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle [*] , signature validation process and any other secure mechanisms if implemented.	
2.12 Verify that firmware can perform automatic firmware updates upon a predefined schedule.	Verification shall be done as per the applicable scenario: Case 1: Automatic OTA updates are available: A standard operating procedure for issuing automatic updates/upgrade s to the in-field	Vendorshallprovidethefollowing:1.Modesofupdatesavailablei.e.automatic,manual or both.2.Organizationalprocessandpoliciesregardingtheissuingofupdatestothedevicesto	
	s to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency as per C20, C21 and C22	devices.	



Public IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 29 of 34

			security requirement. Case 2: Automatic OTA updates are not available and vendor provides manual updates: A standard operating procedure for issuing manual updates/upgrade s to the in-field devices is required to be submitted by the vendor which can		
			by the evaluation agency as per		
			security requirement.		
3.	Secure Process Conformance	3.1 Verify that wireless communica tions are mutually authenticat ed.	Testing, in presence of OEM team, to verify the process of mutual authentication as laid down in the documentation by the vendor.	Vendors shall provide the documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated.	
				In case, the device does not support wireless communications, the vendor shall provide a declaration for the	



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 30 of 34

			same.	
	3.2 Verify	Identifying all the	Vendors shall	
	that	security	provide the	
	wireless	mechanisms	documentation	
	communica	being used in the	regarding the	
	tions are	communication	security measures	
	sent over	process	implemented in the	
	an	verification	device to prevent	
	encrynted	through	tampering of the	
	channel	• Testing in	data heing sent	
	channel.	• Testing, in	through wireless	
		ofOEM	modo of	
			illoue of	
		team	communication.	
		• Lode	In man the let	
		review	in case, the device	
		Process	uoes not support	
		audit of	wireless	
		the key-	communications,	
		life cycle	the vendor shall	
		process	provide a	
			declaration for the	
			same.	
	3.3 Verify		Vendor shall	
	that		submit Bill of	
	whether		materials for	
	trusted		critical hardware	
	sources are		components	
	being used		(related to security	
	for sourcing		functions like SoC).	
	the			
	component			
	s of the			
	device i.e.			
	trusted			
	supply			
	chain			
	through a			
	managed			
	Bill of			
	materials			
	for critical			
	hardware			
	component			
	component			





P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 31 of 34

s (related to		
security		
functions		
like SoC) is		
in use.		
3.4 Supply	Vendor shall	
chain risk	submit the	
identificatio	following:	
n.	Supply chain risk	
assessment.	identification.	
prioritizatio	assessment.	
n. and	prioritization, and	
mitigation	mitigation	
shall be	documents.	
conducted.		
Supply	Supply chain	
chain	risk/business	
risk/busine	continuity planning	
SS	policy documents.	
continuity	plavbooks	
planning	reflecting how to	
policy	handle supply	
documents.	chain disruption.	
playbooks	nost-incident	
reflecting	summary	
how to	documents.	
handle	aocamentor	
supply		
chain		
disruption		
nost-		
incident		
summary		
documents		
need to be		
submitted		
and		
demonstrat		
e the same		
35 Verify	Document for	
the no	Network protocols	
nronrietary	used in the device	
network	asca in the actice.	
network		
protocols		

Public
IoT System Certification Scheme
Issue : 01



P01 — Procedure for CCTV Testing Evaluation and Certification

Date : 21-05-2024

Page : 32 of 34

		are being			
		used in the			
		device. If			
		yes, then			
		complete			
		implementa			
		tion details			
		and the			
		source code			
		for the			
		same shall			
		he			
		provided			
4	Security	4.1 Design		Design and	
	Conformance	and		architecture	
	at product	architectur		documents till the	
	development	e details till		PCBA and SoC	
	stage	the PCBA		level	
	Stuge	and SoC			
		level to be			
		provided to			
		aid in			
		counterfeit			
		mitigation			
		and			
		allu malwara			
		detection			
		4.2 Threat	Dragona and		
		4.2 Inreat	Process and		
		initigation	need to be		
		strategies	need to be		
		for tainted	submitted and		
		and	demonstrate the		
		counterien	same.		
		products			
		shall be			
		implemente			
		d as part of			
		product			
		uevelopme			
		4.3 Une or	List of		
		more up-to-	components that		
		date	have been		
		malware	identified as		



IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01 Date : 21-05-2024

Page : 33 of 34

datastian	requiring			
uetection	requiring			
tools shall	tracking targets			
be	of			
deployed as	tainting/counterf			
nort of the	aiting CM tool			
part of the	eiting, CM tool.			
code	Quality assurance			
acceptance	process need to			
and	be submitted and			
developme	demonstrate the			
uevelopine				
nt	same.			
processes.				
Malware				
detection				
techniques				
chall ho				
Shall De				
used before				
final				
packaging				
and				
deliverv				
(o g				
(e.g.,				
scanning				
finished				
products				
and				
component				
s for				
5 101				
maiware				
using one				
or more up-				
to-date				
malware				
dotoction				
toois j.				
4.4 Supply		Supply chain		
chain risk		risk/business		
identificatio		continuity planning		
n		nolicy documents		
11, 2000000000		poncy uocuments,		
assessment,		piaybooks		
prioritizatio		reflecting how to		
n, and		handle supply		
mitigation		chain disruption,		
			1	1



conducted.	summary	
	documents need to	
	be submitted and	
	demonstrate the	
	same.	